

Das Projekt „Bumblebee“ wird gefördert bzw. finanziert im Rahmen des FTI-Programms FORTE durch das Bundesministerium für Finanzen und von der Österreichischen Forschungsförderungsgesellschaft abgewickelt.



Bumblebee

Studie

Table of Contents

Management Summary	11
1 Einleitung.....	13
2 Scope & Abgrenzung	14
3 Bedarfsanalyse	16
3.1 Einleitung	16
3.2 Zielsetzung.....	18
3.3 Methodisches Vorgehen und Limitationen	20
3.3.1 Methodische Zielsetzung und Forschungslogik	20
3.3.2 Untersuchungsdesign und Datengrundlage.....	21
3.3.3 Qualitative Erhebungen im Projektkontext.....	22
3.3.4 Literatur-, Dokumenten- und Referenzanalyse	24
3.3.5 Auswertungslogik und analytische Kategorien	25
3.3.6 Methodische Triangulation und Qualität der Befunde.....	27
3.3.7 Reichweite und Limitationen der Analyse	29
3.4 Bedarfserhebung	31
3.4.1 Workshop 23.11.2023	31
3.4.2 Workshop 15.12.2023	32
3.4.3 Workshop 08.02.2024	34
3.4.4 Workshop 19.02.2024	36
3.4.5 Aktuelle Ausbildungsstruktur	36
3.5 Identifizierte Herausforderungen und Entwicklungsbedarfe	38
3.5.1 Anforderungen an das Curriculum	38
3.5.2 Organisation und Rahmenbedingungen der Ausbildung	39
3.5.3 Prüfungen und Evaluierung.....	39
3.5.4 Relevanz aktueller Cyberbedrohungen.....	40
3.5.5 Relevante Standards und Rahmenwerke	41
3.5.6 Einordnung der Ergebnisse des Workshops.....	43
3.5.7 Synthese der Bedarfserhebung.....	44
3.6 Vergleich von Cybersicherheitsausbildung im militärischen Sektor.....	46
3.6.1 Ausbildung in Österreich	46
3.6.2 Ausbildung in Deutschland	48
3.6.3 Ausbildung in Estland	49
3.6.4 Ausbildung in Frankreich.....	50
3.6.5 Ausbildung in Italien	51
3.6.6 Ausbildung in Norwegen.....	52
3.6.7 Ausbildung in der Schweiz	53
3.6.8 Ausbildung in den USA.....	54
3.6.9 Ausbildung in Kanada.....	56
3.6.10 Ausbildung im Vereinigten Königreich	57
3.6.11 Vergleichende Einordnung und Implikationen für Bumblebee.....	59
3.7 Relevante Standards und Rahmenwerke für die Cybersicherheitsausbildung.....	62
3.7.1 Militärische Standardisierungsvereinbarungen (STANAG).....	62
3.7.2 ISO/IEC 27000-Serie.....	63
3.7.3 ITIL.....	65
3.7.4 COBIT	67
3.7.5 ENISA	69
3.7.6 NIST Cybersecurity Framework	71

3.7.7	Cybersecurity Body of Knowledge	73
3.7.8	CIS Critical Security Controls	74
3.8	Implikationen für das Projekt Bumblebee	77
3.9	Trainingsplattformen und Cyber-Range-Umgebungen	79
3.9.1	Trainingsplattformen für die Cybersicherheitsausbildung	79
3.9.2	Cyber Ranges als spezialisierte Trainingsumgebungen	81
3.9.3	Beispiele bestehender Cyber Ranges	83
3.9.4	Technologie-Stack von Cyber Ranges	85
3.10	Auswahlkriterien für eine geeignete Trainingsplattform	89
3.11	Implikationen für das Projekt Bumblebee	92
3.12	Parameter und Indikatoren für die Aus- und Fortbildung im militärischen SOC-/NOC-Kontext 94	
3.12.1	Cybersecurity-relevante technische Vermittlung	94
3.12.2	Organisatorisches Design	96
3.12.3	Individuelle Trainingsbedürfnisse	97
3.12.4	Nutzung der Indikatoren für die Evaluierung	99
4	Trainingsumgebung	102
4.1	Scope & Abgrenzung	102
4.2	Anforderungen & Qualitätsziele	104
4.2.1	Stakeholder- und Zielgruppenanalyse	104
4.2.2	Funktionale Anforderungen	106
4.2.3	Nicht-funktionale Anforderungen (Qualitätsattribute)	111
4.2.4	Traceability	114
4.3	Architekturleitlinien & Methodik	129
4.3.1	Zweck, Anwendungsbereich und Geltung	129
4.3.2	Architekturleitlinien (Prinzipien)	129
4.4	Kontext & Use-Cases	131
4.4.1	Methodik	131
4.4.2	Systemkontext	131
4.4.3	Domänenmodell	131
4.4.4	Use-Case	133
4.5	Referenzarchitektur A – VM-zentriert & HLA/DIS-föderiert	145
4.5.1	Übersicht & Bausteine	145
4.5.2	Technologie-Stack und Plattformkomponenten	146
4.5.3	Integrations- & Föderationskonzept	150
4.5.4	Deploy-/Infrastruktur-View	150
4.5.5	IaC & Betriebsartefakte	153
4.5.6	Sicherheit & Betrieb	155
4.5.7	Risiken	157
4.6	Referenzarchitektur B – Cloud-native (Kubernetes) mit Service-Mesh & DDS/HLA-Bridge	162
4.6.1	Übersicht & Bausteine	163
4.6.2	Technologie-Stack und Plattformkomponenten	164
4.6.3	Integrations- & Föderationskonzept	168
4.6.4	Deploy-/Infrastruktur-View	169
4.6.5	IaC & Betriebsartefakte	169
4.6.6	Sicherheit & Betrieb	170
4.6.7	Risiken	172
4.7	Variantenvergleich & Entscheidungsvorlage	177
4.7.1	Entscheidungsrahmen und Fragestellung	177

4.7.2	Kriterienkatalog (mit Operationalisierung).....	177
4.7.3	Gewichtungsbildung	179
4.8	Schnittstellen- & Datenarchitektur	185
4.8.1	Schnittstellen-Übersicht.....	185
4.8.2	Schnittstellen Detailbeschreibungen	187
4.8.3	Datenarchitektur	190
4.9	Sicherheit & Compliance	203
4.9.1	Zonen- und Segmentierungsmodell	203
4.9.2	Identität & Zugriff	205
4.9.3	Härtung der Plattform	207
4.9.4	Schlüsselverwaltung, Rotation, Tresor.....	208
4.9.5	Protokollierung, Observability & Audit.....	210
4.9.6	Policies-as-Code & Compliance-Nachweis.....	211
4.9.7	Unterschiede/„Deltas“ zwischen Referenzarchitektur A und B	211
4.10	Bereitstellung, Betrieb & Support	213
4.10.1	Runbooks	213
4.10.2	Offline-Prozesse	217
4.10.3	SLA/SLOs und Kapazitätsplanung.....	221
4.11	Validierung & Nachweisführung	225
4.11.1	Zielbild und Vorgehensmodell.....	226
4.11.2	Testplan: Funktions-, Integrations-, Last-, Sicherheits- und Föderationstests ...	226
4.11.3	Abnahmekriterien je Anforderung	229
4.11.4	Evidenz, Messdisziplin und Audit.....	231
4.11.5	PoC/MVP-Fahrplan (Iterationen und Meilensteine)	232
4.12	Roadmap & Risiken	235
4.12.1	Zielbild und Annahmen.....	235
4.12.2	Sechs Monate Roadmap zum MVP.....	237
4.12.3	Roadmap – erweiterter Pfad (~12 Monate bis Zielbild)	241
4.12.4	Einführungs- und Migrationsplan	246
4.12.5	Konsolidiertes Risiko-Register mit Gegenmaßnahmen	250
5	Curriculum	256
5.1	Scope & Abgrenzung des Curriculums	258
5.2	Ausgangspunkt	260
5.3	Mission und Zielsetzung	261
5.3.1	Mission des Ausbildungsprogramms	261
5.3.2	Zielsetzung des Curriculums	261
5.3.3	Einordnung in strategische Rahmenbedingungen	263
5.4	Ausbildungsziele	264
5.4.1	Zielbereich 1: Steigerung der Cyber-Awareness in den Streitkräften.....	264
5.4.2	Zielbereich 2: Aufbau und Vertiefung fachlicher Kompetenzen für SOC- und NOC- Personal	265
5.4.3	Zielbereich 3: Verbesserung der Reaktionsfähigkeit und Resilienz	266
5.4.4	Zielbereich 4: Stärkung von Kooperation, Interoperabilität und Führungsfähigkeit	267
5.4.5	Zielbereich 5: Integration organisatorischer, rechtlicher und ethischer Rahmenbedingungen.....	268
5.5	Didaktische Philosophie und Ansatz	271
5.5.1	Grundgedanken der didaktischen Ausrichtung	271
5.5.2	Praxis- und erfahrungsorientierter Ansatz.....	274
5.5.3	Problemorientierte und szenariobasierte Didaktik	276
5.5.4	Holistischer und interdisziplinärer Ansatz	278



5.5.5	Kollaborative, teamorientierte Ausrichtung	280
5.5.6	Aktualitäts- und zukunftsorientierter Ansatz	282
5.5.7	Präsenzorientierung mit Offline-Selbststudium	284
5.5.8	Ethik- und wertebasierte Philosophie	286
5.6	Struktur des Curriculums	289
5.6.1	Didaktische Progression als leitendes Strukturprinzip	289
5.6.2	Die vier Ebenen der Curriculumsstruktur	291
5.6.3	Kompetenzaufbau und Wiederaufnahme zentraler Konzepte	294
5.6.4	Verbindung von Wissensgebieten, Modulen und Qualifikationsstufen	296
5.6.5	Verschränkung von Fachlichkeit und Anwendungsleistung	298
5.6.6	Übergangsorientierung zwischen Ausbildung, Dienstbetrieb und Teamleistung ...	300
5.6.7	Strukturelle Bedeutung für Qualitätssicherung und Weiterentwicklung	302
5.6.8	Schlussfolgerung zur Curriculumsstruktur	304
5.7	Wissensgebiete	306
5.7.1	Systematik der Wissensgebiete	306
5.7.2	Knowledge Areas der Basisausbildung	307
5.7.3	Gemeinsame operationelle Knowledge Areas von SOC und NOC	327
5.7.4	SOC-spezifische Knowledge Areas	348
5.7.5	NOC-spezifische Knowledge Areas	358
5.7.6	Optionale Vertiefungen	364
5.8	Ausbildungsmodule	369
5.8.1	Basismodul	369
5.8.2	SOC Modul	372
5.8.3	NOC Modul	373
5.8.4	Abschlussübungen und Prüfungen	376
5.9	Qualitätssicherung und Weiterentwicklung	379
5.9.1	Grundprinzipien der Qualitätssicherung	379
5.9.2	Evaluations- und Reviewmechanismen	382
5.9.3	Weiterentwicklung, Governance und Lessons Learned	384
6	Durchgeführte Trainings	387
6.1	Einordnung des Evaluationsabschnitts und Projekthintergrund	387
6.2	Evaluationsdesign und methodisches Vorgehen	388
6.2.1	Evaluationsziele	388
6.2.2	Methodischer Ansatz	388
6.2.3	Evaluierungsdimensionen	389
6.2.4	Durchführung der Evaluierung	389
6.3	Übungen	391
6.3.1	Erste Cyber-Übung Februar 2024	391
6.3.2	Zweite Cyber-Übung September 2024	393
6.3.3	Dritte Cyber-Übung Juli 2025	394
6.3.4	Vierte Cyber-Übung März 2026	396
7	Zusammenfassung und Conclusio	399
8	Literaturverzeichnis	400

Abbildungen

Abbildung 1 ITIL V3 SERVICE LIFECYCLE (Quelle: i-doit.com)	67
Abbildung 2 COBIT SCHLÜSSELKOMPONENTE (Quelle: itsm-docs.com)	69
Abbildung 3 NIST RAHMENWERK (QUELLE: NIST.GOV)	72
Abbildung 4 CIS CONTROLS (QUELLE: TRIPWIRE.COM)	76
Abbildung 5 SZENARIO MODELLIEREN & VERSIONIEREN	135
Abbildung 6 SZENARIO PROVISIONIEREN (IAC)	136
Abbildung 7 ÜBUNG STARTEN/STEUERN	137
Abbildung 8 HANDS-ON-LAB ABSOLVIEREN	138
Abbildung 9 FÖDERIERTE ÜBUNG KOPPELN	139
Abbildung 10 REALGERÄT ANBINDEN	140
Abbildung 11 OBSERVABILITY & TRIAGE	141
Abbildung 12 AAR ERZEUGEN & EXPORTIEREN	142
Abbildung 13 ARTEFAKT-SUPPLY OFFLINE	143
Abbildung 14 RESET/RECOVERY/DR	144
Abbildung 15 ARCHITEKTUR A ÜBERSICHT DER BAUSTEINE	146
Abbildung 16 SINGLE-SITE LAB – ZONEN & GUARDS	152
Abbildung 17 MULTI-SITE – FÖDERATIONS-VRF/VPN ZWISCHEN SITES	153
Abbildung 18 ARCHITEKTUR B ÜBERSICHT DER BAUSTEINE	164
Abbildung 19 METAMODELL DER DATENARCHITEKTUR	191
Abbildung 20 RUN-INSTANZ	192
Abbildung 21 TELEMETRIE-INSTANZ	193
Abbildung 22 AAR-MANIFEST PART 1	194
Abbildung 23 AAR-MANIFEST PART 2	194
Abbildung 24 KLASSIFIZIERUNGSMETADATEN (BEISPIEL)	196
Abbildung 25 FÖDERATIONSNACHWEIS OHNE HOCHSTUFUNG DES AAR (BEISPIEL)	197
Abbildung 26 ZONENMODELL	204
Abbildung 27 ZUGRIFFSPROZESS	206
Abbildung 28 Zusammenspiel der Ausbildungsziele	264
Abbildung 29 ENTWICKLUNG VON CYBER-AWARENESS	265
Abbildung 30 STUFENMODELL DER FACHLICHEN KOMPETENZENTWICKLUNG IN SOC UND NOC	266
Abbildung 31 REAKTIONSKETTE UND RESILIENZ IM CYBER- UND INFORMATIONSRaum	267
Abbildung 32 CURRICULUM BASISAUSBILDUNG	307
Abbildung 33 CURRICULUM SOC MODUL 2	308
Abbildung 34 CURRICULUM NOC MODUL 2	308

Tabellen

Tabelle 1 Parameter und Indikatoren matrix	94
Tabelle 2 FUNKTIONALE ANFORDERUNGEN	107
Tabelle 3 NICHT-FUNKTIONALE ANFORDERUNGEN	111
Tabelle 4 REQUIRMENTS TRACABILITY MATRIX (RTM)	115
Tabelle 5 USE CASE ÜBERSICHT	133
Tabelle 6 TECHNOLOGIE-STACK REFERENZARCHITEKTUR (VM-ZENTRIERT)	147
Tabelle 7 RISIKOKATALOG A	158
Tabelle 8 TECHNOLOGIE-STACK REFERENZARCHITEKTUR (CLOUD-NATIVE)	165
Tabelle 9 RISIKOKATALOG B	173
Tabelle 10 SCORE-CARD	178
Tabelle 11 GOVERNANCE RACI	183

Tabelle 12 INTERFACE ÜBERSICHT	185
Tabelle 13 Metastruktur Curriculum	306
Tabelle 14 CURRICULUM MODULSTRUKTUR	307
Tabelle 15 WISSENSEINHEITEN UND THEMEN IDENTITY MANAGEMENT.....	309
Tabelle 16 KERNELEMENTE UND LERNERGEBNISSE IDENTITY MANAGEMENT	309
Tabelle 17 Wissensseinheiten und Themen Awareness and Understanding.....	310
Tabelle 18 Kernelemente und Lernergebnisse Awareness and Understanding	310
Tabelle 19 Wissensseinheiten und Themen Social and Behavioral Privacy.....	311
Tabelle 20 Kernelemente und Lernergebnisse Social and Behavioral Privacy.....	312
Tabelle 21 Wissensseinheiten und Themen Policy and Compliance Management	312
Tabelle 22 Kernelemente und Lernergebnisse Policy and Compliance Management.....	313
Tabelle 23 Wissensseinheiten und Themen Security Governance.....	314
Tabelle 24 Kernelemente und Lernergebnisse Security Governance	314
Tabelle 25 Wissensseinheiten und Themen Compliance Monitoring and Reporting.....	315
Tabelle 26 Kernelemente und Lernergebnisse Compliance Monitoring and Reporting.....	316
Tabelle 27 Wissensseinheiten und Themen Risk Management	317
Tabelle 28 Kernelemente und Lernergebnisse Risk Management.....	317
Tabelle 29 Wissensseinheiten und Themen Cybersecurity Planning	318
Tabelle 30 Kernelemente und Lernergebnisse Cybersecurity Planning	319
Tabelle 31 Wissensseinheiten und Themen Cybersecurity Resilience.....	319
Tabelle 32 Kernelemente und Lernergebnisse Cybersecurity Resilience.....	320
Tabelle 33 Wissensseinheiten und Themen Information and Asset Classification.....	320
Tabelle 34 Kernelemente und Lernergebnisse Information and Asset Classification.....	321
Tabelle 35 Wissensseinheiten und Themen Security Evaluation Models.....	322
Tabelle 36 Kernelemente und Lernergebnisse Security Evaluation Models.....	323
Tabelle 37 Wissensseinheiten und Themen Security Capabilities of Information Systems	323
Tabelle 38 Kernelemente und Lernergebnisse Security Capabilities of Information Systems....	324
Tabelle 39 Wissensseinheiten und Themen Embedded Devices and Cyber-physical System Vulnerability	325
Tabelle 40 Kernelemente und Lernergebnisse Embedded Devices and Cyber-Physical System Vulnerability	325
Tabelle 41 Wissensseinheiten und Themen Data Security	326
Tabelle 42 Kernelemente und Lernergebnisse Data Security	327
Tabelle 43 Gemeinsame Knowledge Areas.....	327
Tabelle 44 Wissensseinheiten und Themen System Thinking.....	328
Tabelle 45 Kernelemente und Lernergebnisse System Thinking	328
Tabelle 46 Wissensseinheiten und Themen System Management	329
Tabelle 47 Kernelemente und Lernergebnisse System Management	330
Tabelle 48 Wissensseinheiten und Themen System Access.....	330
Tabelle 49 Kernelemente und Lernergebnisse System Access.....	331
Tabelle 50 Wissensseinheiten und Themen System Retirement.....	332
Tabelle 51 Kernelemente und Lernergebnisse System Retirement.....	332
Tabelle 52 Wissensseinheiten und Themen System Control.....	333
Tabelle 53 Kernelemente und Lernergebnisse System Control.....	333
Tabelle 54 Wissensseinheiten und Themen System Testing.....	334
Tabelle 55 Kernelemente und Lernergebnisse System Testing.....	335
Tabelle 56 Wissensseinheiten und Themen Secure Network Protocols.....	335
Tabelle 57 Kernelemente und Lernergebnisse Secure Network Protocols.....	336
Tabelle 58 Wissensseinheiten und Themen Fundamentals of SIEM Technology.....	337
Tabelle 59 Kernelemente und Lernergebnisse Fundamentals of SIEM Technology	337
Tabelle 60 Wissensseinheiten und Themen Incident Response and Forensic Analysis	338
Tabelle 61 Kernelemente und Lernergebnisse Incident Response and Forensic Analysis	338
Tabelle 62 Wissensseinheiten und Themen Tool Assistance	339
Tabelle 63 Kernelemente und Lernergebnisse Tool Assistance	340
Tabelle 64 Wissensseinheiten und Themen Security Architecture Vulnerabilities	340
Tabelle 65 Kernelemente und Lernergebnisse Security Architecture Vulnerabilities.....	341



Tabelle 66 Wissenseinheiten und Themen Log Data Analysis Techniques.....	342
Tabelle 67 Kernelemente und Lernergebnisse Log Data Analysis Techniques.....	342
Tabelle 68 Wissenseinheiten und Themen Data Collection and Processing.....	343
Tabelle 69 Kernelemente und Lernergebnisse Data Collection and Processing	343
Tabelle 70 Wissenseinheiten und Themen Data Visualization and Communication	344
Tabelle 71 Kernelemente und Lernergebnisse Data Visualization and Communication	345
Tabelle 72 Wissenseinheiten und Themen Event monitoring and Threat Detection	345
Tabelle 73 Kernelemente und Lernergebnisse Event Monitoring and Threat Detection	346
Tabelle 74 Wissenseinheiten und Themen Cryptography	347
Tabelle 75 Kernelemente und Lernergebnisse Cryptography	347
Tabelle 76 SOC-spezifische Knowledge Areas	348
Tabelle 77 Wissenseinheiten und Themen Threat Intelligence	348
Tabelle 78 Kernelemente und Lernergebnisse Threat Intelligence	349
Tabelle 79 Wissenseinheiten und Themen Anomaly Identification	349
Tabelle 80 Kernelemente und Lernergebnisse Anomaly Identification	350
Tabelle 81 Wissenseinheiten und Themen Conflict and Cyberspace	351
Tabelle 82 Kernelemente und Lernergebnisse Conflict and Cyberspace	351
Tabelle 83 Wissenseinheiten und Themen Information Warfare.....	352
Tabelle 84 Kernelemente und Lernergebnisse Information Warfare.....	352
Tabelle 85 Wissenseinheiten und Themen Situational Picture	353
Tabelle 86 Kernelemente und Lernergebnisse Situational Picture	354
Tabelle 87 Wissenseinheiten und Themen Log Analysis	354
Tabelle 88 Kernelemente und Lernergebnisse Log Analysis	355
Tabelle 89 Wissenseinheiten und Themen Forensic Investigations.....	355
Tabelle 90 Kernelemente und Lernergebnisse Forensic Investigations.....	356
Tabelle 91 Wissenseinheiten und Themen Response to Cyber Interventions.....	357
Tabelle 92 Kernelemente und Lernergebnisse Response to Cyber Interventions.....	357
Tabelle 93 NOC-spezifische Knowledge Areas	358
Tabelle 94 Wissenseinheiten und Themen Network Traffic Analysis.....	358
Tabelle 95 Kernelemente und Lernergebnisse Network Traffic Analysis.....	359
Tabelle 96 Wissenseinheiten und Themen Security Architecture for OT.....	359
Tabelle 97 Kernelemente und Lernergebnisse Security Architecture for OT	360
Tabelle 98 Wissenseinheiten und Themen Security Guidelines and Standards.....	361
Tabelle 99 Kernelemente und Lernergebnisse Security Guidelines and Standards.....	361
Tabelle 100 Wissenseinheiten und Themen Network Traffic Activity Detection and Tracking ...	362
Tabelle 101 Kernelemente und Lernergebnisse Network Traffic Activity Detection and Tracking	363
Tabelle 102 Wissenseinheiten und Themen Detecting CS Attacks	363
Tabelle 103 Kernelemente und Lernergebnisse Detecting CS Attacks	364
Tabelle 104 Optionale Vertiefungen.....	364
Tabelle 105 Wissenseinheiten und Themen Linux	365
Tabelle 106 Kernelemente und Lernergebnisse Linux	365
Tabelle 107 Wissenseinheiten und Themen Penetration Testing Fundamentals	366
Tabelle 108 Kernelemente und Lernergebnisse Penetration Testing Fundamentals	366
Tabelle 109 Wissenseinheiten und Themen Penetration Testing Advanced.....	367
Tabelle 110 Kernelemente und Lernergebnisse Penetration Testing Advanced	368

Abkürzungsverzeichnis

AAR – After-Action Report
ACL – Access Control List
ADR – Architecture Decision Record
AHP – Analytic Hierarchy Process
AIT – Austrian Institute of Technology
AMQP – Advanced Message Queuing Protocol
API – Application Programming Interface
APT – Advanced Persistent Threat
AWS – Amazon Web Services
BKP – Backup
BMQ – Basic Military Qualification
CAFCYBERCOM – Canadian Armed Forces Cyber Command
CAPA – Corrective and Preventive Actions
CCNA – Cisco Certified Network Associate
CCDCOE – Cooperative Cyber Defence Centre of Excellence
CERT – Computer Emergency Response Team
CIA – Confidentiality, Integrity, Availability
CIR – Cyber- und Informationsraum
CIS – Center for Internet Security
CISA – Cybersecurity and Infrastructure Security Agency
CISO – Chief Information Security Officer
CMDB – Configuration Management Database
CNI – Container Network Interface
COBIT – Control Objectives for Information and Related Technologies
COMCYBER – Commandement de la cyberdéfense
Cosign – Sigstore
CR14 – Cyber Range 14
CRATE – Cyber Range and Training Environment
CRD – Custom Resource Definition
CRL – Certificate Revocation List
CS – Committee for Standardization
CSF – Cybersecurity Framework
CSIRT – Computer Security Incident Response Team
CTF – Capture the Flag
CTU – Cyber Training Unit
CSV – Comma-Separated Values
CyBOK – Cyber Security Body of Knowledge
DCO – Defensive Cyberspace Operations
DDS – Data Distribution Service
DDS/HLA-Bridge – DDS↔HLA Mapping
DIS – Distributed Interactive Simulation
DNS – Domain Name System
DR – Disaster Recovery

ECSF – European Cybersecurity Skills Framework
ENISA – European Union Agency for Cybersecurity
EW – Electromagnetic Warfare
FIPS – Federal Information Processing Standards
FOI – Swedish Defence Research Agency
FOM – Federation Object Model
GitOps – Git-getriebener Betriebsstil
GPS – Global Positioning System
gRPC – Remote Procedure Call Framework
GUI – Graphical User Interface
HIL – Hardware-in-the-Loop
HLA – High Level Architecture
HSM – Hardware Security Module
HTB – Hack The Box
IaC – Infrastructure as Code
IAEA – International Atomic Energy Agency
ICS – Industrial Control Systems
IEC – International Electrotechnical Commission
IdP – Identity Provider
IEEE – Institute of Electrical and Electronics Engineers
IG – Implementation Group
IKT – Informations- und Kommunikationstechnologie
IPFIX – IP Flow Information Export
IPsec – Internet Protocol Security
ISACA – Information Systems Audit and Control Association
ISMS – Information Security Management System
ISO – International Organization for Standardization
ISO/IEC – International Organization for Standardization / International Electrotechnical Commission
IT – Informationstechnologie
ITIL – Information Technology Infrastructure Library
JSON – JavaScript Object Notation
JTC – Joint Technical Committee
JYVSECTEC – Jyväskylä Security Technology
K8s – Kubernetes
KIRAS – Sicherheitsforschungsförderprogramm der Republik Österreich
KPI – Key Performance Indicator
Kyverno – (Policy-Engine)
LRS – Learning Record Store
MELT – Metrics, Events, Logs, Traces
MITRE – MITRE Corporation
mTLS – Mutual TLS



MQTT – Message Queuing Telemetry Transport
MVP – Minimum Viable Product
NATO – North Atlantic Treaty Organization
NICCS – National Initiative for Cybersecurity Careers and Studies
NIST – National Institute of Standards and Technology
NOC – Network Operations Center
NSO – NATO Standardization Office
NTNU – Norwegian University of Science and Technology
NTP – Network Time Protocol
OCI – Open Container Initiative
OCO – Offensive Cyberspace Operations
OCSP – Online Certificate Status Protocol
OIDC – OpenID Connect
OPA – Open Policy Agent
OPC UA – Open Platform Communications Unified Architecture
OSINT – Open Source Intelligence
OT – Operational Technology
OTLP – OpenTelemetry Protocol
P95 – 95-Perzentil
Packer – Image-Build-Tool
PDCA – Plan–Do–Check–Act
PDU – Protocol Data Unit
PKI – Public Key Infrastructure
PME – Professional Military Education
PoC – Proof of Concept
PTP – Precision Time Protocol
QoS – Quality of Service
RBAC – Role-Based Access Control
RGCE – Realistic Global Cyber Environment
RMC – Royal Military College of Canada
RPO – Recovery Point Objective
RTO – Recovery Time Objective
RTM – Requirements Traceability Matrix
S3 – (S3-kompatibler) Objekt-Storage
SANS – SysAdmin, Audit, Network and Security
SBOM – Software Bill of Materials
SC 27 – Subcommittee 27
SEC – Security (Prefix)
SEI – Software Engineering Institute
SemVer – Semantic Versioning
SIEM – Security Information and Event Management
SIGINT – Signals Intelligence
SLA – Service Level Agreement
SLO – Service Level Objective
SOM – Simulation Object Model
SOP – Standard Operating Procedure
SOC – Security Operations Center
SPIFFE – Secure Production Identity Framework for Everyone

SPIRE – SPIFFE Runtime Environment
STANAG – Standardization Agreement
SVID – SPIFFE Verifiable Identity Document
SVS – Service Value System
SWEBOK – Software Engineering Body of Knowledge
Syslog – System Logging Protocol
TCP – Transmission Control Protocol
TLS – Transport Layer Security
TPM – Trusted Platform Module
TTP – Tactics, Techniques and Procedures
UMGC – University of Maryland Global Campus
URL – Uniform Resource Locator
USA – United States of America
UTC – Coordinated Universal Time
VLAN – Virtual Local Area Network
VM – Virtuelle Maschine
VPN – Virtual Private Network
VRF – Virtual Routing and Forwarding
WireGuard – (VPN-Protokoll)
WORM – Write Once, Read Many
xAPI – Experience API
YAML – YAML Ain't Markup Language

Spezielle Markierungen aus den Anforderungstabellen:

- [T] – Technische/Engineering-Sicht (System/Plattform).
- [U] – Nutzer:innen-/Didaktik-Sicht (Trainer:innen/Teilnehmende).
- [O] – Organisations-/Betriebs-/Governance-Sicht.

Management Summary

Der vorliegende Endbericht führt die im Projekt Bumblebee erarbeiteten Ergebnisse aus Bedarfsanalyse, Konzeption der Trainingsumgebung, Curriculum-Entwicklung sowie Demonstration und Evaluierung in einem konsistenten Gesamtdokument zusammen. Ziel der Zusammenführung ist es, die fachliche und methodische Entwicklungslinie des Projekts in einer geschlossenen Argumentation sichtbar zu machen: von der systematischen Erhebung des militärischen Ausbildungsbedarfs über die architektonische Konzeption einer geeigneten Trainingsumgebung und die curriculare Ausgestaltung eines SOC-/NOC-orientierten Ausbildungsprogramms bis hin zur empirischen Validierung der entwickelten Inhalte in mehreren Trainingsdurchläufen.

Im ersten Teil wird der Ausbildungsbedarf im militärischen Cyberkontext aus einer mehrperspektivischen Analyse heraus bestimmt. Die Bedarfsanalyse zeigt, dass die Qualifizierung von Personal für SOC- und NOC-nahe Aufgaben nicht auf technisches Spezialwissen reduziert werden kann. Erforderlich ist vielmehr eine integrierte Kompetenzentwicklung, die fachliche, organisatorische, prozessuale und didaktische Anforderungen miteinander verschränkt. Besondere Relevanz besitzen dabei die Fähigkeit zur Früherkennung sicherheitsrelevanter Ereignisse, zur strukturierten Lagebeurteilung, zur regelgeleiteten Eskalation sowie zur nachvollziehbaren Dokumentation und Kommunikation unter den Bedingungen militärischer Organisationen. Zugleich verdeutlicht der internationale Vergleich, dass moderne Cybersicherheitsausbildung in sicherheitskritischen Kontexten zunehmend auf modulare Curricula, praxisnahe Trainingsumgebungen und die Verbindung aus Grundlagenvermittlung, Spezialisierung und simulationsgestützter Anwendung setzt.

Der zweite Teil überführt diese Anforderungen in ein technisches Zielbild für eine integrierte Trainingsumgebung. Das Konzept der Trainingsplattform adressiert die Notwendigkeit, Cyber-Range-Szenarien, Hands-on-Labs, föderierte Übungen und gegebenenfalls Hardware-in-the-Loop-Elemente auf einer gemeinsamen, reproduzierbaren und sicher betreibbaren Grundlage zusammenzuführen. Hervorgehoben wird insbesondere die Eignung einer Plattform, die unter hochsicheren und vorzugsweise vom Internet entkoppelten Bedingungen betrieben werden kann. Durch die Entwicklung zweier Referenzarchitekturen – einer VM-zentrierten und einer cloud-nativen Variante – wird nicht nur eine technische Lösungslandschaft beschrieben, sondern auch ein belastbarer Entscheidungsrahmen bereitgestellt, der Sicherheitsanforderungen, Skalierbarkeit, Betriebsaufwand, Integrationsfähigkeit und Governance-Aspekte systematisch berücksichtigt. Damit wird deutlich, dass die technische Umgebung selbst als didaktisch und organisatorisch wirksamer Bestandteil des Ausbildungsprogramms zu verstehen ist.

Der dritte Teil konkretisiert diese konzeptionellen und technischen Grundlagen in Form eines Curriculums für militärisches SOC- und NOC-Personal. Das Curriculum folgt einem kompetenzorientierten, praxisnahen und spiralförmig aufgebauten Ansatz. Es verbindet Basisausbildung, gemeinsame operationelle Wissensgebiete, rollenbezogene Vertiefungen sowie integrative Abschlussübungen zu einer kohärenten Ausbildungsarchitektur. Von besonderer Bedeutung ist die curriculare Entscheidung, ein gemeinsames begriffliches und prozessuales Fundament mit differenzierten Spezialisierungen für SOC- und NOC-Rollen zu verbinden. Dadurch wird nicht nur die individuelle Qualifizierung unterstützt, sondern auch die Interoperabilität zwischen Rollen, Teams und Organisationsbereichen gestärkt. Praktische Übungen, Szenarien und simulationsgestützte Trainingsformate sind dabei nicht bloßer Zusatz, sondern konstitutiver Bestandteil der Professionalisierung.

Der vierte Teil dokumentiert schließlich die Durchführung und Evaluierung der Trainings. Die vier im Projektverlauf realisierten Cyber-Übungen zeigen, dass die entwickelte Ausbildungslogik iterativ



verfeinert und evidenzbasiert weiterentwickelt werden konnte. Ausgehend von einer frühen Bedarfserhebung über die Erprobung einzelner Module bis hin zur mehrtägigen Abschlussübung mit starkem Praxisfokus wird sichtbar, dass insbesondere szenariobasiertes, anwendungsorientiertes Lernen hohe Relevanz und Akzeptanz besitzt. Zugleich verdeutlichen die Evaluierungsergebnisse, dass strukturierte Grundlagenvermittlung, abgestufte Lernpfade und eine sorgfältig vorbereitete technische Umgebung wesentliche Voraussetzungen für wirksame Trainings im militärischen Cyberbereich darstellen.

In der Gesamtschau zeigt der Endbericht, dass das Projekt Bumblebee eine konsistente Grundlage für die eigenständige, wissenschaftlich fundierte und praxisorientierte Aus- und Fortbildung militärischen Personals im Cyber- und Informationsraum geschaffen hat. Die Verbindung aus Bedarfsanalyse, technischer Konzeption, curricularer Strukturierung und empirischer Validierung ermöglicht einen belastbaren Bezugsrahmen für die weitere Institutionalisierung entsprechender Ausbildungsangebote. Damit leistet das Projekt einen substanziellen Beitrag zur Stärkung militärischer Handlungsfähigkeit, organisationaler Resilienz und professioneller Reaktionsfähigkeit unter den Bedingungen einer zunehmend digitalisierten und durch Cyberbedrohungen geprägten Sicherheitsumgebung.

1 Einleitung

Die Anforderungen an militärische Ausbildung im Cyber- und Informationsraum haben in den vergangenen Jahren deutlich an Komplexität gewonnen. Digitale Infrastrukturen, Führungs- und Kommunikationssysteme sowie netzwerkgestützte operative Fähigkeiten bilden heute einen integralen Bestandteil militärischer Handlungsfähigkeit. Damit steigt zugleich die Notwendigkeit, Personal nicht nur technisch, sondern auch organisatorisch, prozessual und didaktisch angemessen auf die Bearbeitung sicherheitsrelevanter Ereignisse in SOC- und NOC-nahen Kontexten vorzubereiten. Ausbildung in diesem Feld muss daher gleichermaßen auf Wissensvermittlung, Lageverständnis, Handlungssicherheit, Kooperationsfähigkeit und resilientes Handeln unter Unsicherheit zielen.

Der vorliegende Endbericht bündelt die im Projekt Bumblebee entstandenen zentralen Deliverables zu einem zusammenhängenden Gesamtbericht. Er verfolgt das Ziel, die innere Logik des Projekts in einer durchgehenden wissenschaftlichen Darstellung nachvollziehbar zu machen. Diese Logik beginnt mit der Frage nach dem tatsächlichen Ausbildungsbedarf im militärischen Cyberkontext, führt über die Ableitung einer geeigneten technischen Trainingsumgebung und die Entwicklung eines curriculären Rahmens bis hin zur praktischen Erprobung und Evaluierung der entworfenen Inhalte und Formate. Durch diese Zusammenführung wird der Projektverlauf nicht nur dokumentiert, sondern in seiner konzeptionellen Kohärenz sichtbar gemacht.

Die Reihenfolge der nachfolgenden Hauptteile folgt dieser Entwicklungslogik bewusst. Zunächst wird die Bedarfsanalyse dargestellt, da sie die empirische und konzeptionelle Grundlage für alle weiteren Arbeiten bildet. Darauf aufbauend wird das Konzept der Trainingsumgebung beschrieben, in dem die Anforderungen an technische Architektur, Betriebsmodell und Integrationsfähigkeit operationalisiert werden. Im Anschluss folgt das Curriculum, das die fachlichen, didaktischen und organisatorischen Konsequenzen der vorangegangenen Analysen in eine strukturierte Ausbildungsarchitektur überführt. Abschließend werden die durchgeführten Trainings dargestellt, anhand derer die entwickelten Konzepte unter realitätsnahen Bedingungen validiert und weiterentwickelt wurden.

2 Scope & Abgrenzung

Der vorliegende Endbericht bündelt die im Projekt Bumblebee erarbeiteten fachlichen, methodischen, technischen und didaktischen Ergebnisse in einer integrierten Gesamtdarstellung. Der Bericht rekonstruiert die innere Entwicklungslogik des Vorhabens von der Analyse des militärischen Ausbildungsbedarfs über die Ableitung technischer und organisatorischer Anforderungen bis hin zur curriculären Ausgestaltung und ersten empirischen Validierung eines geeigneten Ausbildungsansatzes. Gegenstand des Berichts ist folglich nicht ein einzelnes Produkt oder Teilresultat, sondern die systematische Herleitung, Konzeption, Ausarbeitung und Einordnung eines militärisch anschlussfähigen Ausbildungsmodells für den Cyber- und Informationsraum mit besonderem Fokus auf SOC- und NOC-nahe Rollenprofile. Der sachliche Fokus des Berichts liegt auf jenen Kompetenz- und Handlungsfeldern, die für die Wahrnehmung operativer Aufgaben im Umfeld der Erkennung, Einordnung, Dokumentation und regelgeleiteten Weiterverarbeitung sicherheitsrelevanter Ereignisse von zentraler Bedeutung sind. Im Zentrum stehen damit nicht abstrakte oder ausschließlich technologisch definierte Cyberfähigkeiten, sondern solche Qualifikationsanforderungen, die sich aus konkreten organisatorischen, prozessualen und didaktischen Erfordernissen militärischer Ausbildungs- und Einsatzkontexte ergeben. Der Bericht umfasst die Bedarfsanalyse, die Ableitung von Anforderungen an eine geeignete Trainingsumgebung, die curriculare Strukturierung des Ausbildungsprogramms sowie die Darstellung und Einordnung der im Projektverlauf durchgeführten Trainings- und Evaluationsschritte. Diese Bereiche werden nicht isoliert behandelt, sondern in ihrer wechselseitigen Abhängigkeit analysiert, da die Entwicklung eines tragfähigen Ausbildungsansatzes im militärischen Cyberkontext nur dann überzeugend gelingen kann, wenn fachliche Inhalte, technische Infrastruktur, didaktische Logik und institutionelle Einbettung gemeinsam betrachtet werden.

Der Bericht verfolgt ausdrücklich nicht das Ziel, sämtliche Dimensionen militärischer Cyberfähigkeit vollständig oder abschließend abzubilden. Nicht Gegenstand des Dokuments ist daher eine Behandlung offensiver Cyberoperationen, strategischer Nachrichtengewinnung, vertiefter digitalforensischer Spezialdisziplinen, allgemeiner IT-Berufsausbildung oder organisationsspezifischer Produktschulungen. Ebenso wenig beansprucht der Bericht, die Gesamtheit möglicher militärischer Rollenprofile im Cyber- und Informationsraum auszudifferenzieren oder eine universell gültige Systematik aller cyberbezogenen Qualifikationspfade bereitzustellen. Vielmehr konzentriert sich die Darstellung bewusst auf jene Rollen- und Aufgabenprofile, für die im Rahmen des Projekts ein nachvollziehbarer, praxisrelevanter und institutionell anschlussfähiger Ausbildungsbedarf identifiziert werden konnte. In ähnlicher Weise ist auch die technische Reichweite des Berichts bewusst begrenzt. Die dargestellten Architekturen, Plattformkonzepte und infrastrukturellen Überlegungen dienen der Entwicklung eines belastbaren Referenzrahmens für Trainings- und Übungsumgebungen, nicht jedoch der vollständigen Feinspezifikation einer unmittelbar produktiv einsetzbaren Realumgebung. Der Bericht formuliert damit kein vollständiges Betriebs- oder Beschaffungskonzept im engeren Sinne, sondern beschreibt technische Lösungsräume, Architekturprinzipien, Entscheidungsoptionen und Umsetzungslogiken, die als Grundlage für nachgelagerte Konkretisierung, Erprobung und institutionelle Adaptation dienen können. Die technische Konzeption ist somit als didaktisch und organisatorisch funktionalisierte Referenzarchitektur zu verstehen, deren Wert nicht in der abschließenden Festlegung eines einzigen Zielsystems, sondern in der nachvollziehbaren Herleitung, Vergleichbarkeit und Begründbarkeit unterschiedlicher Gestaltungsoptionen liegt. Auch in methodischer Hinsicht ist der Bericht als konzeptionell fundierte, zugleich aber projektgebundene Darstellung zu lesen. Die dargestellten Ergebnisse basieren auf der Verbindung qualitativer Erhebungen, strukturierter Referenzanalysen, konzeptioneller Verdichtungen und erster empirischer Erprobungen. Daraus

ergibt sich ein belastbarer, jedoch kontextgebundener Erkenntnisrahmen. Der Bericht erhebt daher keinen Anspruch auf statistische Repräsentativität oder uneingeschränkte Übertragbarkeit auf sämtliche militärischen Organisationen, Ausbildungseinrichtungen oder internationalen Sicherheitskontexte. Vielmehr liegt seine Stärke in der systematischen Verknüpfung von Praxisbezug, fachlicher Strukturierung und wissenschaftlicher Anschlussfähigkeit. Die hier entwickelten Schlussfolgerungen sind folglich als fundierte Grundlage für weitere curriculare, organisatorische und technische Entwicklungsprozesse zu verstehen, nicht jedoch als endgültiger Abschluss dieser Entwicklungen.

Die Abgrenzung betrifft darüber hinaus auch den didaktischen Anspruch des Berichts. Dieser liegt nicht in der vollständigen Ausformulierung aller denkbaren Lehr-/Lerninhalte, Prüfungsformen oder Moduldifferenzierungen, sondern in der Entwicklung eines konsistenten Rahmens, aus dem sich solche Elemente begründet ableiten lassen. Der Bericht schafft damit die Voraussetzungen für eine strukturierte Weiterentwicklung des Ausbildungsprogramms, indem er zentrale Kompetenzdimensionen, Gestaltungsprinzipien, infrastrukturelle Anforderungen und Evaluierungslogiken sichtbar macht. Er ersetzt jedoch nicht die nachgelagerte Detailarbeit, die für die konkrete Implementierung in institutionellen Ausbildungskontexten erforderlich ist. Dazu zählen insbesondere die präzise Operationalisierung einzelner Lernziele, die zeitliche Sequenzierung von Modulen, die Erstellung konkreter Lehrmaterialien, die Anpassung an organisationsspezifische Rahmenbedingungen sowie die kontinuierliche Fortschreibung auf Basis neuer technologischer und sicherheitsbezogener Entwicklungen.

Die Reichweite des Berichts ist damit bewusst so gewählt, dass einerseits ein belastbarer konzeptioneller Kern sichtbar wird, andererseits jedoch Raum für spätere Vertiefung, Anpassung und organisationsspezifische Konkretisierung verbleibt. Diese Offenheit ist nicht als Mangel, sondern als notwendige Eigenschaft eines wissenschaftlich fundierten und praxisorientierten Entwicklungsdokuments zu verstehen. Gerade im Feld der Cybersicherheitsausbildung, das durch technologische Dynamik, sich wandelnde Bedrohungslagen und institutionell unterschiedliche Anwendungsbedingungen geprägt ist, wäre ein vermeintlich abschließender oder universalistischer Anspruch weder fachlich angemessen noch praktisch tragfähig. Die vorliegende Abgrenzung dient daher nicht der Einschränkung des Erkenntnisinteresses, sondern der analytischen Schärfung. Sie stellt sicher, dass Bedarfsanalyse, Trainingsumgebung, Curriculum und Evaluierung in einer gemeinsamen, kohärenten Entwicklungslogik gelesen, eingeordnet und bewertet werden können. Darüber hinaus erfüllt die Abgrenzung eine orientierende Funktion für die Rezeption des Berichts. Sie macht deutlich, unter welchen Annahmen die dargestellten Ergebnisse zu verstehen sind, welche Problemstellungen bewusst in den Mittelpunkt gerückt werden und welche Themenfelder aus Gründen der inhaltlichen Fokussierung, der methodischen Belastbarkeit und der projektbezogenen Umsetzbarkeit ausgeklammert bleiben. Dadurch wird Transparenz hinsichtlich des Geltungsbereichs der Aussagen geschaffen und zugleich eine präzisere Einordnung des Beitrags ermöglicht, den das Projekt Bumblebee für die Entwicklung militärischer Cybersicherheitsausbildung leistet. Der Bericht definiert somit einen wissenschaftlich fundierten und praxisorientierten Referenzrahmen, der auf nachhaltige Kompetenzentwicklung, institutionelle Anschlussfähigkeit und schrittweise Weiterentwicklung ausgerichtet ist und gerade in dieser bewusst gesetzten Reichweite seinen zentralen Wert entfaltet.

3 Bedarfsanalyse

Die nachfolgende Bedarfsanalyse bildet den Ausgangspunkt des Gesamtvorhabens. Sie bestimmt den militärischen Ausbildungsbedarf im Cyberkontext nicht nur deskriptiv, sondern als analytische Grundlage für die spätere Ableitung technischer, didaktischer und organisatorischer Entscheidungen. Damit schafft sie den Referenzrahmen, aus dem sowohl Anforderungen an die Trainingsumgebung als auch die Struktur des Curriculums und die Kriterien der späteren Evaluierung hervorgehen.

3.1 Einleitung

In der heutigen vernetzten und digitalisierten Welt stellen kritische Infrastrukturen eine zentrale Voraussetzung für die Stabilität, Resilienz und Funktionsfähigkeit moderner Staaten dar [1]. Sie gewährleisten die Aufrechterhaltung essenzieller gesellschaftlicher, wirtschaftlicher und sicherheitsrelevanter Prozesse und bilden damit eine wesentliche Grundlage staatlicher Handlungsfähigkeit. Besonders im militärischen Bereich kommt diesen Infrastrukturen eine herausgehobene Bedeutung zu, da militärische Führungs-, Kommunikations- und Informationssysteme nicht nur operationelle Prozesse unterstützen, sondern zugleich die Koordination, Entscheidungsfindung und Durchführung nationaler wie internationaler Sicherheitsaufgaben ermöglichen. Die Verfügbarkeit, Integrität und Vertraulichkeit dieser Systeme ist daher von strategischer Relevanz. Mit der fortschreitenden Digitalisierung militärischer Systeme geht jedoch eine zunehmende Abhängigkeit von Informations- und Kommunikationstechnologien einher. Digitale Vernetzung, automatisierte Prozesse, softwaregestützte Führungsunterstützung sowie die Integration unterschiedlicher Plattformen und Sensoren steigern zwar Effizienz, Reaktionsfähigkeit und Interoperabilität, erweitern jedoch gleichzeitig die potenzielle Angriffsfläche. Diese Entwicklung führt dazu, dass militärische Systeme in wachsendem Maße Ziel cyberbasierter Angriffe und Einflussoperationen werden können. Cyberbedrohungen reichen dabei von punktuellen Störungen einzelner Komponenten über Angriffe auf Kommunikations- und Informationsflüsse bis hin zu komplexen, hybriden Operationen, in denen technische, informationelle und organisatorische Schwachstellen systematisch ausgenutzt werden, um kritische Fähigkeiten eines Staates gezielt zu beeinträchtigen. Die Verwundbarkeit militärischer Strukturen ist damit nicht allein technischer Natur, sondern betrifft gleichermaßen organisationale Abläufe, Entscheidungsprozesse und die Fähigkeit zur koordinierten Reaktion unter dynamischen und unsicheren Bedingungen.

Vor diesem Hintergrund gewinnt die Ausbildung von militärischem Personal im Bereich der Cybersicherheit zunehmend an Bedeutung. Die wirksame Bewältigung cyberbezogener Bedrohungslagen setzt voraus, dass Soldatinnen und Soldaten sowie technisches Fachpersonal nicht nur über grundlegendes technisches Wissen verfügen, sondern auch in der Lage sind, sicherheitsrelevante Ereignisse frühzeitig zu erkennen, deren Bedeutung lagegerecht einzuordnen, angemessene Gegenmaßnahmen einzuleiten und Vorfälle strukturiert an spezialisierte Stellen weiterzuleiten. Erforderlich ist somit ein Kompetenzprofil, das technisches Verständnis, analytische Urteilsfähigkeit, prozessuale Handlungssicherheit und kommunikative Anschlussfähigkeit miteinander verbindet. Ausbildung in diesem Kontext ist daher nicht lediglich als Vermittlung isolierter Fachinhalte zu verstehen, sondern als systematische Befähigung zur professionellen Handlung in komplexen, zeitkritischen und sicherheitsrelevanten Einsatzsituationen.

Im Rahmen des Projekts Bumblebee wurde deshalb eine systematische Analyse der Cybersicherheitsdomäne durchgeführt. Ziel dieser Analyse ist es, die Anforderungen an zukünftige Ausbildungsprogramme im militärischen Cyberbereich differenziert zu identifizieren und geeignete didaktische sowie technologische Trainingsmethoden zu untersuchen. Im Mittelpunkt steht dabei

die Frage, welche Wissensbestände, Fähigkeiten und Handlungskompetenzen in einem militärischen Ausbildungsprogramm adressiert werden müssen, damit Personal in SOC-/NOC-nahen Einsatzkontexten sicherheitsrelevante Ereignisse wirksam bearbeiten kann. Die Analyse versteht sich damit nicht nur als Bestandsaufnahme, sondern als konzeptionelle Grundlage für die Entwicklung eines strukturierten, praxisnahen und institutionell anschlussfähigen Ausbildungsansatzes. Ein besonderer Fokus liegt dabei auf dem Einsatz sogenannter Cyber Ranges, die als realitätsnahe Trainingsumgebungen für Cyberübungen dienen und es ermöglichen, Angriffs- und Verteidigungsszenarien unter kontrollierten, aber zugleich praxisnahen Bedingungen zu simulieren [2]. Solche Umgebungen bieten den Vorteil, komplexe technische und organisatorische Zusammenhänge in einer sicheren Lernumgebung erfahrbar zu machen, ohne operative Systeme zu gefährden. Sie schaffen damit die Möglichkeit, nicht nur technisches Wissen anzuwenden, sondern auch Reaktionsmuster, Entscheidungsprozesse, Teamkoordination und Eskalationslogiken unter annähernd realen Bedingungen zu trainieren. Cyber Ranges sind insofern nicht lediglich technische Plattformen, sondern didaktisch bedeutsame Lern- und Erprobungsräume, in denen sich theoretische Inhalte, praktische Anwendung und evaluierbare Kompetenzentwicklung systematisch miteinander verbinden lassen.

Vor diesem Hintergrund besteht eine zentrale Herausforderung nicht allein in der technischen Absicherung militärischer Informations- und Kommunikationssysteme, sondern ebenso in der systematischen Befähigung des dafür eingesetzten Personals. Im Zentrum steht insbesondere die Frage, welche Kompetenzen Angehörige eines militärischen SOC-/NOC-nahen Einsatzumfelds benötigen, um sicherheitsrelevante Ereignisse frühzeitig zu erkennen, lagegerecht zu bewerten, regelkonform zu dokumentieren und an zuständige Stellen weiterzuleiten. Das vorliegende Deliverable adressiert daher sowohl den konkreten Ausbildungsbedarf als auch die Ableitung geeigneter technologischer und didaktischer Rahmenbedingungen für ein entsprechendes Ausbildungsprogramm. Es leistet damit einen Beitrag zur Entwicklung eines fundierten, wissenschaftlich anschlussfähigen und zugleich praxisorientierten Ausbildungsansatzes, der den besonderen Anforderungen militärischer Cybersicherheitskontexte Rechnung trägt.

3.2 Zielsetzung

Das vorliegende Deliverable verfolgt das Ziel, eine fundierte Bedarfs- und Anforderungsanalyse als konzeptionelle Grundlage für die Entwicklung eines militärisch ausgerichteten Ausbildungsprogramms im Bereich der Cybersicherheit zu erarbeiten. Ausgangspunkt ist die Annahme, dass die wirksame Qualifizierung von Personal in sicherheitskritischen militärischen Kontexten nicht allein von der Vermittlung technischer Inhalte abhängt, sondern in gleicher Weise durch organisatorische Einbettung, rollenbezogene Verantwortlichkeiten sowie didaktisch angemessene Lehr- und Lernformate bestimmt wird. Vor diesem Hintergrund steht die Frage im Zentrum, welche fachlichen, organisatorischen und didaktischen Voraussetzungen erfüllt sein müssen, damit Personal in SOC-/NOC-nahen Funktionen sicherheitsrelevante Ereignisse frühzeitig erkennen, systematisch einordnen, nachvollziehbar dokumentieren und entsprechend definierter Prozesse regelgeleitet eskalieren kann.

Die Zielsetzung des Deliverables geht damit über eine rein deskriptive Bestandsaufnahme hinaus. Vielmehr soll ein analytischer Rahmen geschaffen werden, der es ermöglicht, den Ausbildungsbedarf im militärischen Cyberkontext differenziert zu erfassen und in strukturierte Anforderungen zu überführen. Im Mittelpunkt steht folglich nicht nur die Identifikation einzelner Wissens- und Kompetenzfelder, sondern auch deren Verknüpfung mit organisationalen Abläufen, operativen Einsatzlogiken und institutionellen Rahmenbedingungen. Damit trägt die Analyse dem Umstand Rechnung, dass Cybersicherheitskompetenz im militärischen Umfeld als mehrdimensionale Fähigkeit verstanden werden muss, die technisches Verständnis, situatives Urteilsvermögen, prozessuale Handlungssicherheit und kommunikative Anschlussfähigkeit gleichermaßen umfasst.

Die Untersuchung folgt dabei drei miteinander verbundenen Erkenntnisinteressen. Erstens werden Bedrohungslage, Kompetenzanforderungen und organisatorische Rahmenbedingungen der Cybersicherheitsdomäne im militärischen Umfeld analysiert, um die strukturellen Ausgangsbedingungen eines geeigneten Ausbildungsansatzes zu bestimmen. Dabei ist insbesondere zu klären, welche Rollenprofile, Aufgabenbilder und Handlungserfordernisse in SOC-/NOC-nahen Kontexten relevant sind und welche Qualifikationsniveaus für eine wirksame Aufgabenerfüllung vorausgesetzt werden müssen. Zweitens werden bestehende Ausbildungsansätze im internationalen Vergleich betrachtet, um institutionelle, curriculare und didaktische Muster zu identifizieren, die als Referenz- und Orientierungspunkte für die weitere Konzeption dienen können. Der internationale Vergleich dient dabei nicht der unreflektierten Übernahme bestehender Modelle, sondern der systematischen Herausarbeitung übertragbarer Strukturprinzipien, Good Practices und möglicher Grenzen etablierter Ausbildungsansätze. Drittens werden einschlägige Standards, Kompetenzrahmen sowie Trainingsplattformen und Cyber-Range-Ansätze daraufhin analysiert, inwiefern sie als fachliche, curriculare und technologische Bezugspunkte für die Ausgestaltung des Projekts Bumblebee geeignet sind. Im Vordergrund steht hierbei die Frage, wie normative Referenzmodelle, rollenorientierte Kompetenzbeschreibungen und praxisnahe Übungsumgebungen in ein kohärentes Ausbildungskonzept überführt werden können.

Ein wesentliches Anliegen des Deliverables besteht darin, die spätere Entwicklung des Ausbildungsprogramms auf eine nachvollziehbare und belastbare Grundlage zu stellen. Ziel ist daher nicht die Ausarbeitung eines vollständigen Curriculums im engeren Sinne, sondern die Schaffung eines fundierten konzeptionellen Bezugsrahmens, aus dem Lernziele, Kompetenzdimensionen, Modulstrukturen, Trainingsszenarien und Evaluierungsansätze in einem nachgelagerten Schritt systematisch abgeleitet werden können. Die Analyse versteht sich somit als vorbereitende Strukturierungsleistung, die einerseits empirisch erhobene Bedarfe und andererseits fachlich-normative Referenzpunkte zusammenführt. Dadurch soll sichergestellt



werden, dass die spätere curriculare Ausgestaltung nicht ausschließlich erfahrungsbasiert oder technologisch getrieben erfolgt, sondern auf einer methodisch reflektierten Verknüpfung von Praxisanforderungen, wissenschaftlich anschlussfähigen Konzepten und institutionellen Zielsetzungen beruht.

Darüber hinaus ist die Zielsetzung des Deliverables auch in einem breiteren organisationsbezogenen Kontext zu verorten. Die Entwicklung eines militärischen Ausbildungsprogramms im Bereich Cybersicherheit dient nicht allein dem individuellen Kompetenzaufbau einzelner Teilnehmender, sondern ist zugleich als Beitrag zur Stärkung organisationaler Resilienz, zur Standardisierung von Reaktionsabläufen und zur Verbesserung der Interoperabilität zwischen Rollen, Einheiten und Prozessen zu verstehen. Ausbildung wird insofern nicht nur als Mittel der Wissensvermittlung begriffen, sondern als strategisches Instrument zur Befähigung sicherheitsrelevanter Handlungsfähigkeit unter komplexen, dynamischen und potenziell zeitkritischen Bedingungen. Das Deliverable leistet damit einen Beitrag zur systematischen Fundierung eines Ausbildungsansatzes, der technische, organisatorische und didaktische Anforderungen nicht isoliert betrachtet, sondern in ihrer wechselseitigen Verschränkung analysiert und für die weitere Projektentwicklung nutzbar macht.

3.3 Methodisches Vorgehen und Limitationen

Die vorliegende Bedarfs- und Anforderungsanalyse basiert auf einem mehrstufigen methodischen Vorgehen, das qualitative Erhebungen im Projektkontext mit einer strukturierten Analyse externer Referenzquellen verbindet. Ziel dieses methodischen Zugangs ist es, die Anforderungen an ein militärisch ausgerichtetes Ausbildungsprogramm im Bereich der Cybersicherheit nicht ausschließlich aus einer einzelnen Perspektive abzuleiten, sondern praxisnahe Beobachtungen, institutionelle Rahmenbedingungen, internationale Vergleichsperspektiven und fachlich-normative Bezugspunkte systematisch zusammenzuführen. Auf diese Weise soll eine belastbare konzeptionelle Grundlage geschaffen werden, die sowohl den Besonderheiten des militärischen Ausbildungskontexts Rechnung trägt als auch fachlich nachvollziehbar und wissenschaftlich anschlussfähig ist. Das Kapitel erläutert zunächst die methodische Zielsetzung und die Forschungslogik der Untersuchung, beschreibt anschließend das Untersuchungsdesign sowie die zugrunde liegende Datengrundlage und stellt die qualitativen Erhebungen im Projektkontext sowie die ergänzende Literatur-, Dokumenten- und Referenzanalyse dar. Darauf aufbauend werden die Auswertungslogik und die analytischen Kategorien beschrieben, anhand derer die unterschiedlichen Datenquellen zusammengeführt und interpretiert wurden. Abschließend werden die methodische Triangulation als Ansatz zur Erhöhung der Belastbarkeit der Befunde sowie die Reichweite und Limitationen der Analyse reflektiert. Damit schafft das Kapitel die methodische Transparenz, die erforderlich ist, um die nachfolgenden Ergebnisse und Ableitungen nachvollziehbar einordnen zu können.

3.3.1 Methodische Zielsetzung und Forschungslogik

Die vorliegende Bedarfs- und Anforderungsanalyse verfolgt das Ziel, eine belastbare konzeptionelle Grundlage für die Entwicklung eines militärisch ausgerichteten Ausbildungsprogramms im Bereich der Cybersicherheit zu schaffen. Im Unterschied zu evaluativen Untersuchungen, die auf die Überprüfung oder Optimierung bereits bestehender Curricula abzielen, richtet sich der Fokus dieser Analyse auf die vorgelagerte Phase der systematischen Bedarfsbestimmung und Anforderungsmodellierung. Im Zentrum steht somit die Frage, welche fachlichen, organisatorischen, didaktischen und infrastrukturellen Voraussetzungen erfüllt sein müssen, damit ein zielgruppenadäquater, praxisnaher und institutionell anschlussfähiger Ausbildungsansatz für SOC-/NOC-nahe Rollen entwickelt werden kann. Die Untersuchung ist damit als konzeptionell-analytischer Beitrag zur Curriculumsentwicklung zu verstehen, der die Grundlage für nachgelagerte Entscheidungen hinsichtlich Lernzielen, Modularchitektur, Übungsdesign und Evaluierungslogik bereitstellt. Ausgangspunkt der methodischen Überlegungen ist die Annahme, dass Ausbildungsbedarfe im militärischen Cyberkontext nicht als statische oder ausschließlich technisch definierbare Größen verstanden werden können. Vielmehr sind sie das Ergebnis eines komplexen Zusammenwirkens von Bedrohungslagen, institutionellen Aufträgen, operativen Handlungserfordernissen, rollenbezogenen Verantwortlichkeiten sowie didaktischen und organisatorischen Rahmenbedingungen. Daraus ergibt sich die Notwendigkeit, den Untersuchungsgegenstand nicht eindimensional zu fassen, sondern als mehrschichtiges Anforderungsgefüge zu analysieren. Ein Ausbildungsprogramm in diesem Bereich muss daher nicht nur fachliche Wissensbestände adressieren, sondern zugleich prozessuale Handlungssicherheit, organisationsbezogene Orientierung und die Fähigkeit zur regelgeleiteten Einbettung technischer Befunde in militärische Entscheidungs- und Kommunikationsstrukturen fördern.

Methodisch folgt die Analyse einer anwendungsorientierten Forschungslogik, die darauf abzielt, wissenschaftlich nachvollziehbare Erkenntnisgewinnung mit unmittelbarer Praxisrelevanz zu verbinden. Diese Forschungslogik ist insbesondere für Felder geeignet, in denen nicht primär theoretische Modellbildung im Vordergrund steht, sondern die Entwicklung belastbarer Grundlagen

für die Gestaltung konkreter Handlungs- und Ausbildungsformate. Vor diesem Hintergrund werden praxisnahe Erhebungen mit externer Referenzbildung verknüpft, um sowohl die operative Relevanz der identifizierten Bedarfe als auch deren fachliche und institutionelle Anschlussfähigkeit sicherzustellen. Die Analyse bewegt sich damit an der Schnittstelle zwischen empirischer Bedarfserhebung, konzeptioneller Strukturierung und normativer Einordnung. Die methodische Grundannahme besteht darin, dass Ausbildungsanforderungen im militärischen Cyberkontext nicht hinreichend aus einer einzelnen Perspektive abgeleitet werden können. Weder rein erfahrungsbasierte Einschätzungen aus der Ausbildungspraxis noch ausschließlich literatur-, standard- oder modellbasierte Zugänge reichen aus, um die Vielschichtigkeit der Kompetenzanforderungen angemessen zu erfassen. Erfahrungswissen ist zwar unverzichtbar, da es unmittelbaren Zugang zu praktischen Herausforderungen, realen Qualifikationsdefiziten und organisationsbezogenen Erfordernissen bietet; zugleich bleibt es jedoch häufig kontextgebunden, implizit und nur begrenzt systematisiert. Umgekehrt ermöglichen Literatur, Standards und Kompetenzrahmen eine strukturierte fachliche Einordnung, abstrahieren jedoch vielfach von den konkreten Bedingungen militärischer Ausbildungsrealität. Eine methodisch tragfähige Analyse muss daher beide Zugänge miteinander verschränken.

Vor diesem Hintergrund wird eine mehrperspektivische Vorgehensweise gewählt, die empirisch gewonnene Bedarfe mit internationalen Vergleichsmodellen, normativen Rahmenwerken und technologischen Umsetzungsoptionen in Beziehung setzt. Ziel ist es, nicht nur Einzelaspekte zu erfassen, sondern ein konsistentes Gesamtbild der Anforderungen zu entwickeln, das sowohl die praktische Umsetzbarkeit als auch die fachliche Legitimation eines zukünftigen Ausbildungsprogramms stützt. Die Analyse folgt damit einem triangulativen Ansatz, der unterschiedliche Datenquellen, Betrachtungsebenen und Erkenntnisperspektiven bewusst zusammenführt. Durch diese methodische Triangulation soll die Validität der abgeleiteten Ergebnisse erhöht werden, indem Übereinstimmungen, Ergänzungen, aber auch mögliche Spannungen zwischen den einzelnen Quellen sichtbar gemacht und analytisch verarbeitet werden. Der Erkenntniswert dieses Vorgehens liegt insbesondere darin, dass Anforderungen nicht isoliert aus Einzelbeobachtungen oder normativen Setzungen abgeleitet werden, sondern aus der systematischen Verknüpfung unterschiedlicher Evidenzformen hervorgehen. Die Forschungslogik zielt somit auf eine konzeptionelle Verdichtung, in der praktische Bedarfe, institutionelle Rahmenbedingungen und fachliche Referenzmodelle zu einem belastbaren Anforderungsprofil zusammengeführt werden. Dadurch wird eine Grundlage geschaffen, die einerseits hinreichend kontextspezifisch ist, um den Besonderheiten des militärischen Ausbildungsumfelds Rechnung zu tragen, und andererseits hinreichend systematisch, um als nachvollziehbarer Bezugsrahmen für die weitere curriculare Ausarbeitung dienen zu können.

3.3.2 Untersuchungsdesign und Datengrundlage

Das Untersuchungsdesign der vorliegenden Analyse ist mehrstufig angelegt und folgt einem qualitativ-explorativen Zugang, der unterschiedliche Datenquellen und Erhebungsformate miteinander kombiniert. Ziel dieses Designs ist es, den Ausbildungsbedarf im militärischen Cyberkontext nicht ausschließlich abstrakt oder normativ zu bestimmen, sondern auf der Grundlage realitätsnaher Anforderungen, institutioneller Rahmenbedingungen und externer Referenzmodelle systematisch zu rekonstruieren. Die Untersuchung ist damit nicht auf die Generierung statistisch generalisierbarer Aussagen ausgerichtet, sondern auf die Entwicklung eines fachlich fundierten und kontextsensiblen Anforderungsbildes, das als Grundlage für die nachfolgende curriculare Ausarbeitung dienen kann. Die Datengrundlage setzt sich aus mehreren komplementären Quellen zusammen, die unterschiedliche Funktionen innerhalb des Analyseprozesses erfüllen. Einen ersten zentralen Bestandteil bilden qualitative Erhebungen im Projektkontext, insbesondere Workshops, leitfadengestützte Gespräche und eine erste praktische Übung. Diese Formate dienen dazu, Anforderungen aus der Perspektive der militärischen

Ausbildungspraxis sichtbar zu machen und Informationen über bestehende Wissensstände, wahrgenommene Kompetenzbedarfe, organisatorische Abläufe, didaktische Präferenzen sowie technische und infrastrukturelle Voraussetzungen zu gewinnen. Die qualitative Ausrichtung dieser Erhebungen ermöglicht es, insbesondere jene kontextgebundenen und erfahrungsbasierten Aspekte zu erfassen, die in formalen Dokumenten oder standardisierten Modellen häufig nur unzureichend abgebildet sind.

Ein zweiter Bestandteil der Datengrundlage besteht in der Analyse externer Referenzquellen. Hierzu zählen internationale Ausbildungsansätze, einschlägige Standards und Kompetenzrahmen sowie bestehende Trainingsplattformen und Cyber-Range-Konzepte. Diese Materialien wurden herangezogen, um die empirisch erhobenen Bedarfe in einen breiteren fachlichen, institutionellen und technologischen Kontext einzuordnen. Der Einbezug solcher Referenzquellen dient dabei mehreren Zwecken: Zum einen ermöglicht er eine systematische Verortung der identifizierten Anforderungen innerhalb etablierter Diskurse und Strukturmodelle der Cybersicherheitsausbildung. Zum anderen schafft er eine Grundlage dafür, projektspezifische Bedarfe nicht nur aus der Binnenperspektive des eigenen Kontexts zu interpretieren, sondern mit externen Vergleichsmaßstäben abzugleichen und konzeptionell zu schärfen. Das Untersuchungsdesign folgt somit dem Prinzip der komplementären Evidenzbildung. Die im Projektkontext erhobenen Daten liefern unmittelbare Hinweise auf praktische Anforderungen, Zielgruppencharakteristika und institutionelle Rahmenbedingungen. Die externen Referenzquellen tragen demgegenüber dazu bei, diese Beobachtungen systematisch zu strukturieren, zu validieren und in übergeordnete fachliche Zusammenhänge einzuordnen. Die Datengrundlage ist folglich bewusst heterogen angelegt. Diese Heterogenität ist kein methodischer Nachteil, sondern Ausdruck des Untersuchungsziels: Da es nicht um die Prüfung einer eng umrissenen Hypothese, sondern um die Entwicklung eines tragfähigen konzeptionellen Bezugsrahmens geht, ist die Zusammenführung unterschiedlicher Evidenzformen nicht nur sinnvoll, sondern erforderlich. Zugleich ist hervorzuheben, dass die Auswahl der Datengrundlage funktional auf das Erkenntnisinteresse der Untersuchung ausgerichtet ist. Berücksichtigt wurden insbesondere jene Quellen und Erhebungsformate, die Aussagen über operative Kompetenzanforderungen, organisatorische Prozesslogiken, didaktische Gestaltungserfordernisse und technologische Umsetzungsoptionen ermöglichen. Die Datengrundlage ist somit nicht als vollständige Abbildung des gesamten Forschungsfeldes zu verstehen, sondern als gezielt kuratierte Informationsbasis, die für die Entwicklung eines militärisch anschlussfähigen Ausbildungsansatzes im SOC-/NOC-nahen Bereich als besonders relevant erachtet wird. Ihr Erkenntniswert liegt in der Möglichkeit, praxisbezogene und fachlich strukturierte Perspektiven in einer gemeinsamen analytischen Logik zusammenzuführen.

Aus methodischer Sicht ist das Untersuchungsdesign damit als explorativ, anwendungsorientiert und triangulativ zu charakterisieren. Explorativ ist es insofern, als es auf die strukturierte Erschließung eines komplexen und bislang nicht vollständig ausformulierten Anforderungsraums abzielt. Anwendungsorientiert ist es, weil die Erkenntnisgewinnung ausdrücklich auf die spätere Entwicklung eines konkreten Ausbildungsprogramms bezogen bleibt. Triangulativ ist es schließlich deshalb, weil unterschiedliche Datenquellen und Betrachtungsebenen bewusst zusammengeführt werden, um die Belastbarkeit der abgeleiteten Anforderungen zu erhöhen. Auf diese Weise schafft das Untersuchungsdesign die Voraussetzung dafür, Einzelbefunde nicht isoliert zu belassen, sondern in ein kohärentes, fachlich nachvollziehbares und für die weitere Projektentwicklung nutzbares Gesamtbild zu überführen.

3.3.3 Qualitative Erhebungen im Projektkontext

Die qualitativen Erhebungen im Projektkontext bilden den empirischen Kern der vorliegenden Bedarfs- und Anforderungsanalyse. Ihre Funktion besteht darin, jene Anforderungen sichtbar zu

machen, die sich aus der konkreten Ausbildungspraxis, aus organisationsspezifischen Rahmenbedingungen sowie aus den Erwartungen und Vorerfahrungen relevanter Akteursgruppen ergeben. Im Unterschied zu rein dokumentenbasierten oder normativ hergeleiteten Zugängen ermöglichen qualitative Erhebungen einen unmittelbaren Einblick in die tatsächlichen Herausforderungen, Wissensbestände und Handlungslogiken des militärischen Ausbildungsumfelds. Sie sind daher besonders geeignet, um implizites Erfahrungswissen, kontextgebundene Problemwahrnehmungen und praktisch relevante Kompetenzanforderungen systematisch zu erschließen.

Im Rahmen des Projekts kamen hierfür insbesondere Workshops, leitfadengestützte Gespräche und eine erste praktische Übung zum Einsatz. Diese Erhebungsformate wurden gewählt, weil sie unterschiedliche, sich ergänzende Perspektiven auf den Untersuchungsgegenstand eröffnen. Workshops ermöglichen die strukturierte Diskussion von Anforderungen, Bedarfen und Zielvorstellungen in einem interaktiven Setting und fördern die gemeinsame Explikation von Erwartungen, Problemfeldern und Prioritäten. Leitfadengestützte Gespräche bieten demgegenüber die Möglichkeit, Einschätzungen einzelner Beteiligter vertieft zu erfassen und insbesondere jene Aspekte sichtbar zu machen, die in Gruppensettings unter Umständen weniger deutlich artikuliert werden. Die ergänzende praktische Übung erfüllt schließlich eine explorative Funktion, indem sie erste Hinweise darauf liefert, wie sich angenommene Kompetenzanforderungen, didaktische Herausforderungen und technische Voraussetzungen unter handlungsnahen Bedingungen manifestieren.

Ein besonderer Erkenntniswert der qualitativen Erhebungen liegt darin, dass sie nicht nur deklaratives Wissen über Ausbildungsbedarfe erfassen, sondern auch strukturelle und prozessuale Bedingungen der Ausbildung sichtbar machen. So können etwa Unterschiede im Vorwissen der Zielgruppe, Anforderungen an die zeitliche und organisatorische Einbettung der Ausbildung, Vorstellungen über geeignete Lehr-/Lernformate oder die praktische Relevanz bestimmter Inhalte und Werkzeuge differenziert herausgearbeitet werden. Auf diese Weise entsteht ein Bedarfsbild, das nicht allein auf abstrakten Kompetenzmodellen basiert, sondern an den tatsächlichen Bedingungen der späteren Ausbildungsumsetzung orientiert ist. Gerade im militärischen Kontext, in dem Ausbildung stets in institutionelle Strukturen, Rollenlogiken und geregelte Kommunikations- und Eskalationsprozesse eingebettet ist, stellt dies einen wesentlichen methodischen Vorteil dar. Darüber hinaus tragen qualitative Erhebungen dazu bei, die Zielgruppe des geplanten Ausbildungsprogramms nicht als homogene Einheit zu behandeln, sondern in ihrer inneren Differenziertheit wahrzunehmen. Unterschiedliche Vorkenntnisse, Rollenprofile, Erwartungshaltungen und Handlungsspielräume beeinflussen maßgeblich, welche Inhalte vermittelt werden sollten, auf welchem Komplexitätsniveau dies sinnvoll ist und welche didaktischen Zugänge sich für die Zielgruppe als angemessen erweisen. Die qualitativen Erhebungen ermöglichen es daher, den Ausbildungsbedarf nicht nur inhaltlich, sondern auch adressatenbezogen zu strukturieren. Dies ist besonders relevant für ein Ausbildungskonzept, das nicht primär auf hochspezialisierte Expertinnen und Experten, sondern auf operativ handlungsfähiges Personal in SOC-/NOC-nahen Rollen abzielt.

Methodisch ist zugleich zu berücksichtigen, dass qualitative Erhebungen interpretativen Charakter besitzen. Sie liefern keine statistisch repräsentativen Aussagen über sämtliche potenziellen Zielgruppen oder institutionellen Kontexte, sondern verdichtete Einsichten in wahrgenommene Bedarfe, Problemlagen und Anforderungen innerhalb des konkreten Projektzusammenhangs. Ihr wissenschaftlicher Wert liegt daher nicht in quantitativer Verallgemeinerbarkeit, sondern in der strukturierten Rekonstruktion relevanter Perspektiven und in der Generierung kontextsensibler Erkenntnisse. Diese Erkenntnisse gewinnen ihre Belastbarkeit insbesondere dadurch, dass sie im weiteren Verlauf der Analyse mit externen Referenzquellen, internationalen Vergleichsperspektiven und normativen Rahmenwerken in Beziehung gesetzt werden. Die

qualitativen Erhebungen sind somit nicht als isolierter Untersuchungsschritt zu verstehen, sondern als integraler Bestandteil eines mehrperspektivischen Forschungsdesigns. Sie schaffen die empirische Grundlage dafür, praktische Anforderungen, institutionelle Rahmenbedingungen und didaktische Erfordernisse nicht nur abstrakt zu postulieren, sondern aus der Perspektive realer Ausbildungskontexte zu rekonstruieren. Dadurch leisten sie einen zentralen Beitrag zur Entwicklung eines Anforderungsprofils, das sowohl fachlich tragfähig als auch operativ anschlussfähig ist und somit als fundierte Ausgangsbasis für die nachgelagerte Curriculumsentwicklung im Projekt Bumblebee dienen kann.

3.3.4 Literatur-, Dokumenten- und Referenzanalyse

Die qualitativen Erhebungen im Projektkontext wurden durch eine strukturierte Literatur-, Dokumenten- und Referenzanalyse ergänzt, um die empirisch identifizierten Bedarfe fachlich einzuordnen, konzeptionell zu verdichten und mit etablierten externen Bezugsrahmen in Beziehung zu setzen. Diese Analyseebene erfüllt im Gesamtaufbau der Untersuchung eine doppelte Funktion: Einerseits dient sie der Kontextualisierung der im Projekt erhobenen Anforderungen, andererseits ermöglicht sie die Prüfung, inwiefern bestehende Modelle, Standards und Ausbildungsansätze als Orientierungspunkte für die Entwicklung des Projekts Bumblebee herangezogen werden können. Die Untersuchung folgt damit der Annahme, dass praxisnahe Bedarfe erst dann in belastbare curriculare Anforderungen überführt werden können, wenn sie nicht isoliert betrachtet, sondern mit fachlich etablierten Wissensbeständen, normativen Strukturierungsangeboten und technologischen Umsetzungsmodellen abgeglichen werden.

Im Rahmen der Literatur- und Dokumentenanalyse wurden unterschiedliche Quellentypen berücksichtigt, die jeweils spezifische Erkenntnisfunktionen erfüllen. Dazu zählen zunächst wissenschaftliche und fachbezogene Publikationen, die einen Überblick über Kompetenzanforderungen, Ausbildungslogiken und didaktische Herausforderungen im Bereich der Cybersicherheitsausbildung bieten. Ergänzend wurden institutionelle und normative Dokumente analysiert, insbesondere Standards, Frameworks und Kompetenzmodelle, die Rollenprofile, Sicherheitsprozesse, Governance-Aspekte oder inhaltliche Wissensbereiche systematisieren. Darüber hinaus wurden Beschreibungen und Dokumentationen bestehender Trainingsplattformen, Laborumgebungen und Cyber-Range-Konzepte einbezogen, um technologische und didaktische Umsetzungsmöglichkeiten für den identifizierten Ausbildungsbedarf zu untersuchen. Ein zentraler Bestandteil dieser Analyse war der internationale Vergleich bestehender Ausbildungsansätze im militärischen oder sicherheitsnahen Umfeld. Ziel dieses Vergleichs war nicht die Bewertung einzelner nationaler Modelle im Sinne einer normativen Rangordnung, sondern die strukturierte Identifikation wiederkehrender Muster, institutioneller Lösungen und curricularer Prinzipien. Von besonderem Interesse waren dabei Fragen nach dem Verhältnis von technischer Spezialisierung und organisatorischer Einbettung, nach der institutionellen Verankerung von Cyberausbildung, nach der Modularität und Stufung von Ausbildungsangeboten sowie nach dem Stellenwert praxisnaher Übungs- und Simulationsformate. Der internationale Vergleich ermöglicht es damit, projektspezifische Überlegungen in eine breitere Perspektive einzubetten und zugleich jene Strukturprinzipien zu identifizieren, die unter Berücksichtigung des eigenen Kontexts als übertragbar erscheinen.

Die Analyse einschlägiger Standards und Kompetenzrahmen diene vor allem der fachlichen Strukturierung der erhobenen Bedarfe. Solche Referenzmodelle bieten nicht nur terminologische und konzeptionelle Klarheit, sondern ermöglichen auch eine systematische Zuordnung von Rollen, Aufgabenfeldern, Kompetenzdimensionen und Prozessanforderungen. Für die Entwicklung eines militärisch ausgerichteten Ausbildungsprogramms ist dies insofern relevant, als die spätere Curriculumsentwicklung nicht allein an situativen Bedarfen ausgerichtet sein sollte, sondern an fachlich anschlussfähigen Ordnungsmustern, die Transparenz, Nachvollziehbarkeit und

Vergleichbarkeit unterstützen. Die Einbeziehung von Standards und Kompetenzrahmen dient somit nicht der mechanischen Übernahme externer Vorgaben, sondern ihrer reflektierten Nutzung als Strukturierungs- und Orientierungsinstrumente. Ein weiterer Fokus der Referenzanalyse lag auf bestehenden Trainingsplattformen und Cyber-Range-Ansätzen. Dabei wurde untersucht, welche funktionalen, didaktischen und infrastrukturellen Eigenschaften solche Umgebungen aufweisen und inwiefern sie geeignet sind, die im Projekt identifizierten Ausbildungsziele zu unterstützen. Im Vordergrund stand nicht die isolierte Bewertung einzelner Technologien, sondern die Frage, welche Formen digitaler Lern- und Übungsinfrastrukturen notwendig sind, um Kompetenzen im Bereich der Ereigniserkennung, Erstbewertung, Dokumentation, Kommunikation und Eskalation praxisnah zu vermitteln. Die Analyse solcher Plattformen erlaubt es, technologische Optionen nicht losgelöst von didaktischen Anforderungen zu betrachten, sondern als Teil eines integrierten Ausbildungssystems, in dem Lernziele, Szenarien, Rollenlogiken und technische Umsetzungsbedingungen aufeinander abgestimmt sein müssen. Methodisch ist die Literatur-, Dokumenten- und Referenzanalyse als strukturierende und kontextualisierende Ergänzung der qualitativen Erhebungen zu verstehen. Ihr Wert liegt insbesondere darin, dass sie die im Projekt identifizierten Beobachtungen in größere fachliche, institutionelle und technologische Zusammenhänge einordnet. Dadurch wird verhindert, dass die Analyse auf eine rein binnenperspektivische Betrachtung des eigenen Projektkontexts beschränkt bleibt. Gleichzeitig trägt die Referenzanalyse dazu bei, die abgeleiteten Anforderungen begrifflich zu präzisieren, konzeptionell zu ordnen und im Hinblick auf ihre curriculare und technologische Umsetzbarkeit zu überprüfen. Sie leistet damit einen wesentlichen Beitrag zur wissenschaftlichen Fundierung der Untersuchung.

Zugleich ist zu betonen, dass die Funktion der Literatur- und Dokumentenanalyse nicht in der bloßen Zusammenstellung externer Modelle oder Praxisbeispiele besteht. Entscheidend ist vielmehr deren analytische Verarbeitung im Hinblick auf die spezifische Fragestellung des Projekts. Die herangezogenen Referenzen werden daher nicht als normativ verbindliche Blaupause verstanden, sondern als konzeptionelle Bezugspunkte, deren Relevanz jeweils im Lichte des militärischen Ausbildungskontexts, der Zielgruppe und der identifizierten Bedarfe zu prüfen ist. Die Analyse verfolgt somit einen selektiv-reflexiven Zugang: Externe Modelle werden daraufhin befragt, welche Elemente für den Aufbau eines operativ anschlussfähigen, didaktisch tragfähigen und institutionell integrierbaren Ausbildungsansatzes nutzbar gemacht werden können. Insgesamt trägt die Literatur-, Dokumenten- und Referenzanalyse dazu bei, die empirischen Befunde des Projekts Bumblebee in einen übergeordneten fachlichen Zusammenhang einzubetten und dadurch die Belastbarkeit der späteren Anforderungsableitung zu erhöhen. Sie schafft eine Verbindung zwischen projektinterner Bedarfserhebung und externer Wissensordnung und ermöglicht es, praktische Beobachtungen in systematisch strukturierte curriculare Überlegungen zu überführen. Damit bildet sie einen unverzichtbaren Bestandteil des methodischen Gesamtansatzes und unterstützt die Zielsetzung, ein Ausbildungskonzept nicht nur praxisnah, sondern auch fachlich nachvollziehbar und wissenschaftlich anschlussfähig zu fundieren.

3.3.5 Auswertungslogik und analytische Kategorien

Die Auswertung der im Rahmen der Untersuchung erhobenen und analysierten Materialien erfolgte entlang eines kategoriegeleiteten, strukturierenden Vorgehens, das darauf ausgerichtet ist, heterogene Datenquellen in einer gemeinsamen analytischen Logik zusammenzuführen. Ziel dieses Auswertungsschritts war es, die aus qualitativen Erhebungen, Literatur- und Dokumentenanalysen sowie Referenzmodellen gewonnenen Einzelbefunde nicht isoliert nebeneinander stehen zu lassen, sondern in ein konsistentes Anforderungsprofil zu überführen. Die Auswertungslogik folgt damit dem Anspruch, unterschiedliche Perspektiven auf den Untersuchungsgegenstand so zu ordnen, dass aus einer Vielzahl einzelner Beobachtungen,

Einschätzungen und Referenzen systematisch verwertbare Aussagen für die spätere Curriculumsentwicklung abgeleitet werden können.

Ausgangspunkt der analytischen Verdichtung ist die Annahme, dass Ausbildungsanforderungen im militärischen Cyberkontext mehrdimensional strukturiert sind. Sie betreffen nicht ausschließlich fachlich-technische Wissensbestände, sondern ebenso organisatorische Einbettung, prozessuale Handlungssicherheit, didaktische Vermittlungslogiken sowie technische und infrastrukturelle Voraussetzungen der Ausbildungsumsetzung. Um dieser Mehrdimensionalität methodisch Rechnung zu tragen, wurden vier zentrale analytische Kategorien definiert: technische Kompetenzanforderungen, organisatorische Prozessanforderungen, didaktische Anforderungen sowie infrastrukturelle Rahmenbedingungen. Diese Kategorien dienen als strukturierendes Raster, innerhalb dessen unterschiedliche Befunde systematisch geordnet, verglichen und in ihren Wechselwirkungen analysiert werden können.

Die Kategorie der technischen Kompetenzanforderungen umfasst jene Wissens- und Fähigkeitsbereiche, die für die Wahrnehmung SOC-/NOC-naher Aufgaben im Kontext sicherheitsrelevanter Ereignisse erforderlich sind. Hierzu zählen insbesondere grundlegende Kenntnisse zu Netzwerken, Systemarchitekturen, Betriebssystemen, Protokollen und sicherheitsrelevanten Angriffsmustern sowie der Umgang mit Monitoring-, Analyse- und Dokumentationswerkzeugen. Entscheidend ist dabei nicht nur das Vorhandensein isolierten Fachwissens, sondern die Fähigkeit, technische Beobachtungen in einem operativen Kontext einzuordnen, relevante von irrelevanten Ereignissen zu unterscheiden und auf dieser Grundlage sachgerechte erste Handlungsschritte einzuleiten. Die technische Dimension ist somit nicht rein instrumentell zu verstehen, sondern als Voraussetzung für eine belastbare Lageeinschätzung im Rahmen definierter Rollen und Prozesse.

Die Kategorie der organisatorischen Prozessanforderungen bezieht sich auf jene Strukturen und Abläufe, innerhalb derer technische Kompetenzen wirksam werden müssen. Im militärischen Kontext ist Cybersicherheitskompetenz stets in institutionelle Verantwortungszusammenhänge eingebettet und kann daher nicht unabhängig von Rollenverständnissen, Meldewegen, Kommunikationsstrukturen und Eskalationsmechanismen betrachtet werden. Zu dieser analytischen Dimension zählen folglich Anforderungen an die regelgeleitete Dokumentation von Ereignissen, an die prozesssichere Weitergabe von Informationen, an das Verständnis für Schnittstellen zwischen unterschiedlichen Funktionen sowie an die Einbettung technischer Befunde in organisationsspezifische Entscheidungs- und Reaktionslogiken. Diese Kategorie ist von zentraler Bedeutung, da sie verdeutlicht, dass operative Handlungsfähigkeit im Cyberbereich nicht allein aus technischem Können resultiert, sondern aus der Fähigkeit, dieses Können in geregelte institutionelle Prozesse zu integrieren.

Die didaktischen Anforderungen bilden eine weitere eigenständige Auswertungskategorie, da die Wirksamkeit eines Ausbildungsprogramms nicht allein von der Auswahl relevanter Inhalte, sondern in erheblichem Maße auch von deren adressatengerechter Vermittlung abhängt. Im Rahmen der Analyse wurden daher jene Aspekte systematisch berücksichtigt, die die Gestaltung der Ausbildung aus pädagogisch-didaktischer Perspektive betreffen. Dazu zählen unter anderem das Verhältnis von Theorie und Praxis, die Sequenzierung von Lerninhalten, die Berücksichtigung heterogener Eingangsvoraussetzungen, die Auswahl geeigneter Übungs- und Prüfungsformate sowie die Frage, in welcher Weise realitätsnahe Szenarien, Gruppenformate oder simulationsbasierte Lernsettings zur Kompetenzentwicklung beitragen können. Die didaktische Dimension ist insofern zentral, als sie die Brücke zwischen identifiziertem Ausbildungsbedarf und tatsächlicher Lernwirksamkeit herstellt. Sie sorgt dafür, dass fachlich relevante Inhalte nicht nur bestimmt, sondern in eine Form überführt werden, die für die Zielgruppe anschlussfähig, motivierend und lernwirksam ist.

Die vierte Kategorie betrifft die infrastrukturellen Rahmenbedingungen der Ausbildungsdurchführung. Darunter fallen jene technischen, organisatorischen und ressourcenbezogenen Voraussetzungen, die erfüllt sein müssen, damit ein identifizierter Ausbildungsbedarf überhaupt in praktikable Lehr-/Lernformate übersetzt werden kann. Hierzu zählen unter anderem verfügbare Plattformen, Simulations- und Laborumgebungen, Zugangs- und Sicherheitsanforderungen, Wartbarkeit, Skalierbarkeit, zeitliche und räumliche Einbettung sowie die Kompatibilität mit bestehenden Ausbildungsstrukturen. Die infrastrukturelle Dimension ist insbesondere im Bereich der Cybersicherheitsausbildung von hoher Relevanz, da viele Lernziele auf realitätsnahe Übungsumgebungen, kontrollierte technische Szenarien und spezifische Interaktionsformen angewiesen sind. Die Analyse berücksichtigt daher nicht nur, welche Inhalte vermittelt werden sollen, sondern auch, unter welchen materiellen und organisatorischen Bedingungen dies überhaupt sinnvoll und nachhaltig möglich ist.

Die Auswertungslogik ist jedoch nicht als starres Klassifikationsschema zu verstehen. Vielmehr wurden die vier Kategorien als analytische Heuristik eingesetzt, um Zusammenhänge, Überschneidungen und Wechselwirkungen zwischen unterschiedlichen Anforderungsdimensionen sichtbar zu machen. In der praktischen Analyse zeigte sich, dass einzelne Befunde häufig mehreren Kategorien zugleich zuzuordnen sind. So besitzt etwa der Umgang mit SIEM-Umgebungen eine technische Dimension, ist zugleich aber eng mit didaktischen Anforderungen an Übungsdesign und mit organisatorischen Anforderungen an Dokumentation und Eskalation verknüpft. Ebenso lässt sich die Relevanz praxisnaher Übungsszenarien nicht ausschließlich didaktisch deuten, sondern steht auch in einem unmittelbaren Zusammenhang mit infrastrukturellen Möglichkeiten und operativen Prozessanforderungen. Die Auswertung zielte daher nicht auf eine künstliche Trennung der Befunde, sondern auf deren strukturierte Verknüpfung. Durch diese kategoriegeleitete Auswertung konnte ein Analyserahmen geschaffen werden, der sowohl die Komplexität des Untersuchungsgegenstands abbildet als auch eine systematische Verdichtung der Ergebnisse ermöglicht. Die analytischen Kategorien fungieren dabei nicht nur als Ordnungsschema für die Auswertung, sondern zugleich als Brücke zur späteren Anforderungsdefinition. Sie erleichtern es, identifizierte Bedarfe in curriculare, organisatorische und technologische Gestaltungsentscheidungen zu überführen und schaffen damit eine nachvollziehbare Verbindung zwischen empirischer Erhebung, konzeptioneller Analyse und praktischer Umsetzungsperspektive.

Somit dient die Auswertungslogik somit der methodisch kontrollierten Überführung heterogener Einzelbefunde in ein konsistentes Gesamtbild. Sie trägt dazu bei, die Untersuchung nicht auf eine lose Sammlung von Beobachtungen zu reduzieren, sondern aus den verschiedenen Evidenzquellen ein strukturiertes Anforderungsprofil abzuleiten, das sowohl wissenschaftlich plausibel als auch für die weitere Entwicklung des Projekts Bumblebee praktisch nutzbar ist.

3.3.6 Methodische Triangulation und Qualität der Befunde

Die vorliegende Untersuchung folgt einem methodischen Triangulationsansatz, um die Belastbarkeit der abgeleiteten Anforderungen zu erhöhen und die Analyse nicht auf eine einzelne Datenquelle oder Perspektive zu stützen. Unter methodischer Triangulation wird in diesem Zusammenhang die bewusste Kombination unterschiedlicher Erhebungs- und Analysezugänge verstanden, die es ermöglicht, einen komplexen Untersuchungsgegenstand aus mehreren Blickwinkeln zu erschließen. Für die vorliegende Bedarfs- und Anforderungsanalyse bedeutet dies, dass qualitative Erhebungen im Projektkontext, externe Referenzanalysen, internationale Vergleichsperspektiven sowie die Betrachtung technologischer Umsetzungsoptionen nicht getrennt nebeneinanderstehen, sondern systematisch aufeinander bezogen werden. Ziel dieses Vorgehens ist es, die Validität der Ergebnisse dadurch zu stärken, dass Übereinstimmungen, Ergänzungen und mögliche Spannungen zwischen unterschiedlichen Evidenzformen sichtbar

gemacht und analytisch verarbeitet werden. Die Relevanz eines solchen Vorgehens ergibt sich insbesondere aus der Beschaffenheit des Untersuchungsgegenstands. Ausbildungsanforderungen im militärischen Cyberkontext sind durch eine hohe Komplexität, Kontextabhängigkeit und Dynamik gekennzeichnet. Sie betreffen nicht nur technische Wissensbestände, sondern ebenso organisationale Verfahren, rollenbezogene Verantwortlichkeiten, didaktische Gestaltungsfragen und infrastrukturelle Umsetzungsbedingungen. Eine isolierte Betrachtung einzelner Teilaspekte würde daher notwendigerweise zu verkürzten Ergebnissen führen. Die Triangulation dient vor diesem Hintergrund dazu, den Untersuchungsgegenstand in seiner Mehrdimensionalität adäquat zu erfassen und die abgeleiteten Anforderungen nicht nur aus einer einzelnen Logik heraus zu begründen, sondern aus der Verschränkung komplementärer Perspektiven.

Ein wesentlicher Vorteil dieses Ansatzes liegt in der Möglichkeit der wechselseitigen Absicherung unterschiedlicher Befundtypen. So können etwa in Workshops und Gesprächen artikuliert Bedarfe mit Standards, Kompetenzrahmen und internationalen Ausbildungsmodellen abgeglichen werden, um zu prüfen, inwiefern sie sich in etablierten fachlichen Strukturierungen wiederfinden oder von diesen abweichen. Ebenso können technologisch orientierte Überlegungen zu Plattformen und Cyber Ranges daraufhin befragt werden, ob sie den empirisch ermittelten didaktischen und organisatorischen Anforderungen tatsächlich entsprechen. Die Triangulation erfüllt damit eine doppelte Funktion: Sie dient einerseits der Plausibilisierung empirischer Beobachtungen und andererseits der kritischen Prüfung externer Referenzmodelle im Hinblick auf ihre Anwendbarkeit im spezifischen Projektkontext.

Die Qualität der Befunde bemisst sich in dieser Untersuchung folglich nicht an statistischer Repräsentativität, sondern an der Nachvollziehbarkeit, Konsistenz und konzeptionellen Tragfähigkeit der Ableitungen. Maßgeblich ist, ob es gelingt, aus unterschiedlichen Materialien ein kohärentes Anforderungsprofil zu entwickeln, das sowohl praxisnah als auch fachlich begründet ist. Ein zentrales Gütekriterium besteht daher in der inneren Kohärenz der Analyse: Einzelbefunde aus verschiedenen Datenquellen müssen nicht identisch sein, sollten sich jedoch in einer Weise ergänzen oder kontrastieren lassen, die zur Schärfung des Gesamtverständnisses beiträgt. Gerade dort, wo unterschiedliche Quellen zu ähnlichen Schlussfolgerungen führen, kann von einer erhöhten Belastbarkeit der Befunde ausgegangen werden. Wo hingegen Divergenzen sichtbar werden, liegt der Erkenntniswert nicht in ihrer Auflösung um jeden Preis, sondern in ihrer analytischen Explikation, da solche Spannungen häufig auf kontextspezifische Bedingungen, Zielkonflikte oder offene Gestaltungsfragen hinweisen. Ein weiteres Qualitätsmerkmal liegt in der transparenten Strukturierung des Analyseprozesses. Die Einteilung der Befunde in analytische Kategorien und ihre systematische Rückbindung an die Zielsetzung der Untersuchung ermöglichen es, aus einer Vielzahl von Einzelbeobachtungen nachvollziehbare Schlussfolgerungen abzuleiten. Qualität entsteht in diesem Zusammenhang nicht allein durch die Menge der herangezogenen Informationen, sondern vor allem durch deren reflektierte Auswahl, konzeptionelle Verdichtung und argumentativ schlüssige Verknüpfung. Die methodische Triangulation dient somit nicht lediglich der Akkumulation von Daten, sondern ihrer kontrollierten Integration in einen belastbaren analytischen Rahmen. Zugleich ist hervorzuheben, dass die Qualität der Befunde wesentlich von der interpretativen Leistung der Analyse abhängt. Die Zusammenführung unterschiedlicher Datenquellen erzeugt keine Objektivität im mechanischen Sinne, sondern erhöht die Belastbarkeit der Ergebnisse dadurch, dass verschiedene Perspektiven zueinander in Beziehung gesetzt und kritisch reflektiert werden. Daraus folgt, dass die Güte der Untersuchung nicht zuletzt von der Plausibilität der Interpretationen, der Stringenz der Argumentation und der Offenlegung methodischer Annahmen abhängt. Die Triangulation ersetzt daher nicht die Notwendigkeit analytischer Sorgfalt, sondern setzt diese vielmehr voraus.

3.3.7 Reichweite und Limitationen der Analyse

Trotz ihres mehrperspektivischen und methodisch triangulativen Zuschnitts ist die vorliegende Analyse in ihrer Reichweite bewusst begrenzt. Sie ist als konzeptionelle Grundlage für die Entwicklung eines militärisch ausgerichteten Ausbildungsprogramms im Bereich der Cybersicherheit angelegt und erhebt daher weder den Anspruch auf eine vollständige Abbildung sämtlicher militärischer Cyberfähigkeiten noch auf eine abschließende curriculare Ausdifferenzierung aller potenziell relevanten Kompetenzfelder. Ihr Erkenntnisinteresse ist gezielt auf jene Anforderungen gerichtet, die für die Konzeption eines operativ anschlussfähigen Ausbildungsansatzes im SOC-/NOC-nahen Umfeld von zentraler Bedeutung sind. Die Ergebnisse sind folglich als strukturierte und fachlich fundierte Grundlage für nachgelagerte Entwicklungsentscheidungen zu verstehen, nicht jedoch als erschöpfende Beschreibung des gesamten militärischen Cyberausbildungsraums. Die inhaltliche Reichweite der Untersuchung ist insbesondere dadurch bestimmt, dass der Fokus auf Rollenprofilen und Handlungskontexten liegt, in denen die Erkennung, Einordnung, Dokumentation und regelgeleitete Eskalation sicherheitsrelevanter Ereignisse im Vordergrund stehen. Betrachtet werden damit vor allem jene Kompetenzanforderungen, die für operative Erstreaktions- und Unterstützungsfunktionen relevant sind und in enger Verbindung zu SOC-/NOC-nahen Tätigkeitsfeldern stehen. Nicht Gegenstand der Analyse sind demgegenüber hochspezialisierte Teilbereiche wie vertiefte digitale Forensik, Malware-Analyse auf Expertenniveau, sicherheitsbezogene Softwareentwicklung, offensive Cyberoperationen, strategische Cyberplanung oder komplexe Intelligence-orientierte Auswertungsfunktionen. Diese Felder weisen eigene Wissensordnungen, methodische Anforderungen und infrastrukturelle Voraussetzungen auf, die im Rahmen der vorliegenden Untersuchung weder inhaltlich noch methodisch adäquat hätten abgedeckt werden können. Die vorgenommene Fokussierung stellt daher keine inhaltliche Leerstelle im engeren Sinne dar, sondern eine bewusste Eingrenzung des Untersuchungsgegenstands im Interesse analytischer Schärfe und praktischer Anschlussfähigkeit.

Eine weitere Limitation ergibt sich aus der qualitativen und kontextgebundenen Anlage der Untersuchung. Die Analyse stützt sich auf praxisnahe Erhebungen, projektbezogene Beobachtungen sowie die Einordnung externer Referenzmodelle. Daraus folgt, dass die abgeleiteten Anforderungen eng mit den Perspektiven der im Projektkontext einbezogenen Akteurinnen und Akteure, mit den institutionellen Rahmenbedingungen des Untersuchungsfeldes sowie mit den ausgewählten Vergleichs- und Referenzquellen verknüpft sind. Die Befunde besitzen insofern einen hohen konzeptionellen und praxisbezogenen Wert, sind jedoch nicht im Sinne statistischer Repräsentativität oder uneingeschränkter Übertragbarkeit zu interpretieren. Ihre Stärke liegt gerade in der kontextsensiblen Rekonstruktion relevanter Anforderungen; zugleich ist zu berücksichtigen, dass andere militärische Organisationen, Einsatzlogiken oder Ausbildungsstrukturen zu abweichenden Schwerpunktsetzungen führen könnten. Auch die Auswahl und Nutzung externer Referenzquellen ist mit spezifischen Einschränkungen verbunden. Internationale Ausbildungsmodelle, Standards, Kompetenzrahmen und technologische Plattformansätze bieten wertvolle Orientierungspunkte, sind jedoch nicht ohne Weiteres auf den spezifischen Kontext des Projekts übertragbar. Zum einen beruhen sie auf unterschiedlichen institutionellen, organisatorischen und rechtlichen Voraussetzungen, zum anderen folgen sie teilweise anderen Ausbildungszielen, Rollenverständnissen oder sicherheitspolitischen Rahmenbedingungen. Die herangezogenen Referenzen konnten daher nicht als direkt übernehmbare Modelle verstanden werden, sondern lediglich als strukturierende und vergleichende Bezugspunkte. Daraus ergibt sich die methodische Notwendigkeit, externe Modelle stets im Lichte des eigenen Projektkontexts kritisch zu prüfen. Die Aussagekraft der Analyse liegt somit nicht in der Übernahme bestehender Best Practices, sondern in deren reflektierter Übersetzung in ein kontextspezifisches Anforderungsprofil.

Eine zusätzliche Begrenzung ergibt sich aus der Dynamik des Untersuchungsfeldes selbst. Der Bereich der Cybersicherheit ist durch rasche technologische Entwicklungen, sich wandelnde Bedrohungslagen, veränderte Angriffsmuster sowie fortlaufende Anpassungen organisatorischer und regulatorischer Rahmenbedingungen gekennzeichnet. Ausbildungsanforderungen sind daher nicht als statische Größen zu verstehen, sondern unterliegen kontinuierlicher Veränderung. Dies betrifft sowohl die technischen Inhalte als auch die Relevanz bestimmter Werkzeuge, Prozesse und Kompetenzprofile. Die im Rahmen dieser Analyse formulierten Anforderungen besitzen daher den Charakter eines belastbaren, aber zeitgebundenen Orientierungsrahmens. Ihre längerfristige Gültigkeit hängt davon ab, inwieweit sie im weiteren Projektverlauf überprüft, aktualisiert und an veränderte Rahmenbedingungen angepasst werden. Darüber hinaus ist zu betonen, dass die vorliegende Untersuchung zwar eine Grundlage für curriculare Entscheidungen schafft, jedoch nicht mit der eigentlichen Curriculumsentwicklung gleichzusetzen ist. Sie formuliert Anforderungen, priorisiert Handlungsfelder und strukturiert relevante Gestaltungsdimensionen, ersetzt jedoch nicht die nachgelagerte Ausarbeitung konkreter Lernziele, didaktischer Sequenzierungen, Modulbeschreibungen, Prüfungsformate oder Evaluierungsinstrumente. Zwischen Anforderungsanalyse und curricularem Design besteht somit ein notwendiger Übergangsschritt, in dem die hier entwickelten Befunde in operationalisierbare Ausbildungsbausteine übersetzt werden müssen. Die Aussagekraft der Analyse ist daher wesentlich auf ihre Funktion als konzeptionelle Vorstrukturierung bezogen.

Trotz dieser Limitationen stellt die Untersuchung eine belastbare Grundlage für die weitere Projektentwicklung dar. Ihre Stärke liegt nicht in dem Anspruch auf Vollständigkeit, sondern in der methodisch reflektierten Eingrenzung des Gegenstands, in der systematischen Verknüpfung unterschiedlicher Evidenzquellen und in der Entwicklung eines Anforderungsprofils, das sowohl fachlich nachvollziehbar als auch praktisch anschlussfähig ist. Die Reichweite der Analyse ist somit bewusst so gewählt, dass sie einerseits hinreichend spezifisch bleibt, um konkrete curriculare und technologische Implikationen zu ermöglichen, andererseits aber offen genug ist, um im weiteren Projektverlauf präzisiert, erweitert und an neue Erkenntnisse angepasst werden zu können. Gerade in dieser Balance zwischen analytischer Fokussierung und konzeptioneller Offenheit liegt ihr zentraler Beitrag für die Entwicklung des Projekts Bumblebee.

3.4 Bedarfserhebung

Die Bedarfserhebung bildet den empirischen Kern der vorliegenden Analyse. Ziel dieses Untersuchungsschritts war es, die Anforderungen an ein zukünftiges militärisch ausgerichtetes Ausbildungsprogramm im Bereich der Cybersicherheit nicht ausschließlich aus Literatur, Standards und bestehenden Referenzmodellen abzuleiten, sondern diese durch die systematische Einbindung relevanter Akteursgruppen praxisnah zu fundieren. Damit folgt das Kapitel der Annahme, dass die Entwicklung eines belastbaren Ausbildungskonzepts nur dann gelingen kann, wenn fachliche, organisatorische, didaktische und infrastrukturelle Anforderungen aus dem realen Anwendungskontext heraus rekonstruiert und in strukturierter Form aufbereitet werden. Zu diesem Zweck wurden mehrere Workshops, Befragungen und eine erste praktische Übung mit Angehörigen der Zielgruppe sowie mit im militärischen Ausbildungsumfeld tätigen Personen durchgeführt. Die Auswertung der hierbei gewonnenen Erkenntnisse erfolgte entlang jener Dimensionen, die bereits im methodischen Teil als zentrale analytische Kategorien definiert wurden: fachliche Kompetenzanforderungen, organisatorische Rahmenbedingungen, didaktische Anforderungen sowie technische und infrastrukturelle Voraussetzungen. Auf diese Weise konnte ein Anforderungsbild entwickelt werden, das sowohl die Perspektive der Auszubildenden als auch jene der potenziellen Teilnehmenden berücksichtigt und dadurch eine evidenzbasierte Grundlage für die spätere Curriculumsentwicklung schafft. Im Rahmen der Bedarfserhebung wurden vier zentrale Erhebungsformate durchgeführt. Dazu zählen ein erster explorativer Workshop zur Analyse des bestehenden Ausbildungsangebots und zur Identifikation grundlegender Anforderungen an einen Cybersecurity-Kurs, ein vertiefender Workshop zu Bedrohungslage, Infrastruktur und Incident-Response-Prozessen, eine erste Cyberübung mit Angehörigen der Zielgruppe einschließlich einer begleitenden Erhebung zum Ausbildungsstatus sowie ein weiterer Workshop mit Auszubildenden im IT-Bereich zur Präzisierung organisatorischer und inhaltlicher Anforderungen. Die nachfolgenden Unterkapitel stellen die wesentlichen Ergebnisse dieser Erhebungen dar und leiten daraus erste Implikationen für die Konzeption des Ausbildungsprogramms ab.

3.4.1 Workshop 23.11.2023

Der Workshop vom 23. November 2023 diente der Analyse der gegenwärtigen Ausbildungssituation im Bereich der Cybersicherheit im militärischen Umfeld sowie der Identifikation erster grundlegender Anforderungen an ein zukünftiges Ausbildungsprogramm. Im Mittelpunkt standen dabei sowohl organisatorische als auch didaktische Fragestellungen, die für die Konzeption eines zielgerichteten Cybersecurity-Kurses von Bedeutung sind. Ziel war es, ein erstes gemeinsames Verständnis darüber zu entwickeln, welche strukturellen Defizite im bestehenden Ausbildungsangebot bestehen und welche Merkmale ein zukünftiger Kurs aufweisen sollte, um den spezifischen Anforderungen des militärischen Kontexts gerecht zu werden.

Die Diskussion machte deutlich, dass im Bereich der militärischen Cybersicherheitsausbildung bislang nur in begrenztem Umfang strukturierte und systematisch aufeinander abgestimmte Ausbildungsangebote vorhanden sind. Daraus ergibt sich ein klarer Bedarf nach einem formalisierten und didaktisch kohärenten Ausbildungskonzept, das sowohl technische Grundkompetenzen als auch organisatorische Handlungslogiken im Umgang mit Cybervorfällen vermittelt. Besonders hervorgehoben wurde die Notwendigkeit einer praxisorientierten Ausgestaltung, die den Teilnehmenden nicht nur theoretisches Grundlagenwissen vermittelt, sondern sie zugleich in die Lage versetzt, sicherheitsrelevante Ereignisse zu erkennen, erste Einschätzungen vorzunehmen, relevante Informationen strukturiert zu dokumentieren und Vorfälle an zuständige Stellen weiterzuleiten.

Im Rahmen des Workshops wurden mehrere grundlegende Anforderungen an einen zukünftigen Kurs identifiziert. So wurde zunächst festgehalten, dass die Kurssprache Deutsch sein sollte, um eine möglichst niederschwellige und zielgruppenadäquate Vermittlung sicherzustellen. Darüber hinaus wurde die Notwendigkeit eines strukturierten Lehrplans betont, der sowohl klar definierte Teilnahmevoraussetzungen als auch nachvollziehbare Prüfungsanforderungen umfasst. Gleichzeitig wurde empfohlen, auf verpflichtendes Vorwissen im Bereich der Cybersicherheit zu verzichten, um auch Teilnehmende mit unterschiedlichen technischen Hintergründen in das Ausbildungsformat einbeziehen zu können. Diese Öffnung erscheint insbesondere vor dem Hintergrund der heterogenen Zielgruppe als sinnvoll, da sie eine breitere Einbindung ermöglicht und den Aufbau eines gestuften Ausbildungskonzepts unterstützt.

Hinsichtlich des Ausbildungsziels bestand Einigkeit darüber, dass der Kurs nicht auf die Ausbildung hochspezialisierter Fachkräfte abzielen sollte, sondern auf die Befähigung von Personal, Cyberangriffe auf Systeme frühzeitig zu erkennen, erste Analysen durchzuführen, relevante Informationen strukturiert zu erfassen und diese an spezialisierte Fachstellen weiterzuleiten. Diese Zielsetzung verweist auf ein Qualifikationsprofil, das im Bereich der operativen Erstreaktion und der prozesssicheren Eskalation verortet ist. Zugleich wurde eine Kursdauer von etwa zwei bis drei Wochen als realistisch und angemessen eingeschätzt. Didaktisch wurde eine Kombination aus theoretischen Grundlagen und praktischen Übungen als besonders geeignet angesehen, da nur durch diese Verknüpfung sowohl ein konzeptionelles Verständnis als auch anwendungsorientierte Handlungssicherheit aufgebaut werden kann. Für die Gruppengröße wurde ein Rahmen von etwa zehn bis fünfzehn Teilnehmenden als zweckmäßig beschrieben, um insbesondere in praxisorientierten Übungsphasen eine angemessene Betreuung zu gewährleisten.

Von besonderer Bedeutung ist schließlich die Feststellung, dass ein zukünftiges Ausbildungsprogramm vor allem auf den Aufbau grundlegender Fähigkeiten in den Bereichen Angriffserkennung, strukturierte Vorfalldokumentation und regelgeleitete Weiterleitung ausgerichtet sein sollte. Damit markiert der Workshop bereits früh eine wesentliche konzeptionelle Leitlinie des Projekts: Im Vordergrund steht nicht die Ausbildung spezialisierter Cyber-Forensikerinnen oder -Forensiker, sondern die Entwicklung eines Ausbildungsangebots, das Teilnehmende zur sicheren Wahrnehmung operativer Erstreaktionsaufgaben befähigt. Die im Workshop gewonnenen Erkenntnisse bilden somit eine wesentliche Ausgangsbasis für die weiteren Erhebungen und die nachfolgende curriculare Verdichtung.

3.4.2 Workshop 15.12.2023

Der Workshop vom 15. Dezember 2023 diente der vertieften Erhebung von Anforderungen an ein zukünftiges Ausbildungsprogramm im Bereich der Cybersicherheit. Im Zentrum standen dabei die aktuelle Bedrohungslandschaft, die Relevanz militärischer und technischer Infrastrukturen sowie organisatorische Abläufe im Bereich Incident Response. Der Workshop zielte darauf ab, die im ersten Erhebungsformat identifizierten Grundanforderungen weiter zu präzisieren und um jene Aspekte zu ergänzen, die sich aus realistischen Bedrohungsszenarien, prozessualen Rahmenbedingungen und den Anforderungen militärischer Kommunikations- und Eskalationsstrukturen ergeben.

Aus Sicht der Ausbilder wurde hervorgehoben, dass ein zukünftiges Ausbildungsprogramm in erster Linie grundlegende Fähigkeiten zur Erkennung und ersten Einordnung von Cyberangriffen vermitteln sollte. Im Vordergrund steht demnach nicht die tiefgehende technische Detailanalyse einzelner Angriffe, sondern die Fähigkeit, potenziell sicherheitsrelevante Ereignisse frühzeitig zu identifizieren, in ihrer möglichen Tragweite einzuschätzen und entsprechend vorgegebener Prozesse korrekt zu eskalieren. Diese Schwerpunktsetzung ist für die spätere Curriculumsentwicklung besonders relevant, da sie die Ausbildung klar auf ein operatives Rollenverständnis ausrichtet, in dem die frühe Erkennung, strukturierte Dokumentation und

prozesssichere Weiterleitung von Vorfällen im Zentrum stehen. Darüber hinaus wurde betont, dass Ausbildungsinhalte eng an realistischen und zeitgemäßen Bedrohungsszenarien orientiert sein sollten. Als besonders relevante Themen wurden hybride Kriegsführung, Desinformationskampagnen und Deepfake-Technologien genannt. Die Aufnahme solcher Phänomene in das Ausbildungsprogramm erscheint insbesondere deshalb sinnvoll, weil moderne Konflikt- und Informationsräume zunehmend durch hybride und informationsbezogene Einflussnahmen geprägt sind. Damit erweitert sich das Verständnis sicherheitsrelevanter Ereignisse über klassische technische Angriffe hinaus und verweist auf die Notwendigkeit, auch jene Bedrohungsformen in die Ausbildung einzubeziehen, die im Grenzbereich zwischen technischer Cyberbedrohung, Informationsmanipulation und operativer Beeinflussung angesiedelt sind.

Ein weiterer Schwerpunkt lag auf der Vermittlung strukturierter Incident-Response-Prozesse. In diesem Zusammenhang wurde empfohlen, sich an etablierten Prozessmodellen zu orientieren, etwa an ITIL-bezogenen Vorgehensweisen oder am PDCA-Zyklus, um standardisierte und nachvollziehbare Abläufe im Umgang mit Sicherheitsvorfällen zu fördern. Diese Orientierung an etablierten Prozessmodellen ist für den militärischen Ausbildungskontext insofern bedeutsam, als sie eine Brücke zwischen technischer Ereignisbehandlung und organisatorischer Prozesssicherheit schlägt. Ergänzend wurde betont, dass Teilnehmende über grundlegende Netzwerkkenntnisse verfügen sollten. Als Referenzrahmen wurde ein Niveau genannt, das sich an elementaren CCNA-Grundlagen orientiert, insbesondere im Hinblick auf Netzwerke, Routing und zentrale Infrastrukturkomponenten. Daraus lässt sich ableiten, dass technische Grundlagen im Bereich Netzwerkverständnis eine wesentliche Voraussetzung für das erfolgreiche Absolvieren weiterführender Inhalte darstellen. Aus Sicht der potenziellen Auszubildenden wurde insbesondere die Bedeutung praxisorientierter Ausbildungsformate hervorgehoben. Die Teilnehmenden sollen reale Angriffsszenarien nachvollziehen und anhand konkreter Fallbeispiele lernen, wie Cybervorfälle erkannt, dokumentiert und kommunikativ weiterverarbeitet werden können. Daraus folgt die Notwendigkeit, mit realitätsnahen Trainingsumgebungen zu arbeiten, in denen typische militärische IT-Infrastrukturen simuliert werden können. Genannt wurden dabei insbesondere Netzwerkkomponenten wie Router und Switches, Firewall-Systeme, Systeme zur Anomalieerkennung sowie militärische Kommunikationssysteme. Der Wert solcher Umgebungen liegt darin, dass sie den Teilnehmenden nicht nur isoliertes Technikwissen vermitteln, sondern ein besseres Verständnis für jene Systeme schaffen, die auch im realen militärischen Einsatzumfeld eine Rolle spielen.

Aus organisatorischer Sicht wurde im Workshop betont, dass Cybervorfälle in militärischen Kontexten innerhalb klar definierter Kommunikations- und Eskalationsstrukturen behandelt werden müssen. In einem möglichen Szenario würde eine Person vor Ort zunächst einen potenziellen Angriff erkennen und in weiterer Folge einen First Responder kontaktieren, der beispielsweise im Cybersicherheitszentrum des Bundesheeres oder im Abwehramt verortet sein könnte. Diese Rolle übernimmt sodann die weitere Analyse und Koordination erforderlicher Maßnahmen. Zugleich wurde deutlich, dass insbesondere in Auslandseinsätzen auch vor Ort technische Ansprechpartner erforderlich sein können, die erste Maßnahmen unter Anleitung durchführen können. Daraus ergibt sich die didaktische und curriculare Anforderung, nicht nur technische Erstreaktionen zu vermitteln, sondern auch die Kommunikation zwischen dezentralen Einsatzräumen und zentralen Stellen unter verschiedenen Rahmenbedingungen vorzubereiten.

In diesem Zusammenhang wurde darauf hingewiesen, dass die Kommunikation je nach Lage über unterschiedliche Kanäle erfolgen kann, etwa über Telefon, Satellitentelefon, Internetverbindungen oder andere militärische Kommunikationssysteme. Ein zentrales Element der Ausbildung sollte daher auch darin bestehen, Verfahren für jene Situationen zu vermitteln, in denen zentrale IT-Systeme oder Netzverbindungen nur eingeschränkt oder gar nicht verfügbar sind. Ebenso wurde

betont, dass im Fall eines Cyberangriffs auch Maßnahmen wie das Isolieren oder temporäre Abschalten eines Netzwerks in Betracht gezogen werden können, um eine weitere Ausbreitung des Angriffs zu verhindern. Die Person vor Ort soll folglich dazu befähigt werden, mögliche Angriffe zu erkennen, erste Gegenmaßnahmen einzuleiten, ein einfaches Lagebild zu erstellen, relevante Ereignisse strukturiert zu dokumentieren und den Vorfall an zuständige Stellen weiterzuleiten. Ein weiterer inhaltlicher Schwerpunkt des Workshops war die Frage nach der Relevanz kritischer Infrastrukturkomponenten. Besonders hervorgehoben wurden militärische Kommunikationsnetze sowie technische Kommunikationssysteme wie das Technical Communication Network. Für Trainingszwecke wurde zugleich festgehalten, dass ausschließlich synthetische oder simulierte Daten verwendet werden sollten und der Einsatz klassifizierter Daten in Ausbildungsumgebungen nicht vorgesehen ist. Diese Festlegung ist für die spätere Gestaltung von Trainingsinfrastrukturen von hoher Bedeutung, da sie klare Anforderungen an Datensicherheit, Szenariendesign und technische Umsetzung formuliert. Schließlich befasste sich der Workshop auch mit der Gestaltung zukünftiger Cyberübungen. Vorgeschlagen wurde die Entwicklung eines strukturierten Handbuchs für Angriffsszenarien, das unterschiedliche Angriffstypen, deren Klassifikation sowie mögliche Reaktions- und Eskalationsmaßnahmen beschreibt. Ein solches Handbuch könnte dazu beitragen, Vorfälle systematisch nach Typ, Schadenspotenzial, Dringlichkeit und möglichen Reaktionsstrategien zu ordnen und damit eine einheitlichere Ausbildungs- und Übungsgrundlage zu schaffen. Zusätzlich wurde empfohlen, auch Kommunikationsszenarien in zukünftige Übungen zu integrieren, etwa die Simulation eines Anrufs bei einer zentralen Stelle. Dadurch könnten Teilnehmende lernen, welche Stelle kontaktiert werden muss, welche Informationen unter den gegebenen Rahmenbedingungen weitergegeben werden dürfen und über welche Kommunikationskanäle ein Bericht erfolgen kann. Insgesamt verdeutlicht der Workshop, dass ein wirksames Ausbildungsprogramm technische, organisatorische und kommunikative Komponenten in enger Verzahnung behandeln muss.

3.4.3 Workshop 08.02.2024

Im Rahmen des Workshops vom 8. Februar 2024 wurde eine erste Cyberübung mit Angehörigen der Zielgruppe durchgeführt, um neben der Erprobung eines initialen Übungsformats auch empirische Erkenntnisse für die Bedarfsanalyse des geplanten Ausbildungsprogramms zu gewinnen. Die Veranstaltung fand in der Landesverteidigungsakademie statt und war als ganztägiges Format konzipiert, das theoretische Einführungselemente mit einer praktischen Übungsphase kombinierte. Insgesamt nahmen zwanzig Personen teil. Ziel des Workshops war es, ein differenzierteres Verständnis für die Vorkenntnisse, Erwartungen, Interessen und didaktischen Präferenzen der Zielgruppe zu entwickeln und zugleich zu beobachten, wie realistische Angriffsszenarien von den Teilnehmenden aufgenommen und bearbeitet werden.

Die Übung umfasste am Vormittag eine Einführung in grundlegende Konzepte der Incident Response sowie eine Vorbereitung auf die Trainingsumgebung. Am Nachmittag wurden drei praktische Angriffsszenarien durchgeführt, darunter Website Defacement, Phishing beziehungsweise Data Leak sowie Remote Code Execution. Diese Szenarien dienten nicht nur der ersten praktischen Erprobung eines möglichen Ausbildungsformats, sondern auch der Beobachtung, inwieweit die Teilnehmenden in der Lage waren, konkrete Analyse- und Reaktionsaufgaben unter praxisnahen Bedingungen zu bewältigen. Damit übernahm die Übung eine doppelte Funktion: Sie war zugleich didaktischer Testlauf und empirisches Erhebungsinstrument.

Die begleitende Erhebung unter den Teilnehmenden zeigte zunächst, dass die Zielgruppe hinsichtlich ihrer Vorkenntnisse deutlich heterogen zusammengesetzt war. Etwa die Hälfte der Teilnehmenden verfügte bereits über erste Erfahrungen im Bereich Cybersicherheit, während die andere Hälfte eher dem Einsteigerbereich zugeordnet werden konnte. Diese Heterogenität ist für

die spätere Curriculumsentwicklung von zentraler Bedeutung, da sie darauf hinweist, dass ein einheitlich voraussetzungsreiches Ausbildungsformat der Zielgruppe nur bedingt gerecht würde. Vielmehr spricht der Befund für ein gestuftes Ausbildungskonzept, das unterschiedliche Eingangsniveaus berücksichtigt und sowohl Teilnehmende mit Vorerfahrung als auch Personen mit geringerem Vorwissen angemessen adressiert. Auch hinsichtlich des Bildungsniveaus zeigte sich eine differenzierte Zusammensetzung. Zwar waren überwiegend Personen mit Matura vertreten, vereinzelt nahmen jedoch auch Personen mit Pflichtschul- oder Lehrabschluss teil. Dieser Befund unterstreicht die Notwendigkeit, Inhalte verständlich, anschlussfähig und praxisnah zu vermitteln, ohne dabei den fachlichen Anspruch grundsätzlich zu reduzieren. Vielmehr ergibt sich hieraus die didaktische Anforderung, komplexe technische und organisatorische Inhalte so aufzubereiten, dass sie für heterogene Lerngruppen zugänglich bleiben.

Inhaltlich zeigte die Erhebung, dass die stärksten Interessen der Teilnehmenden in den Bereichen System- und Netzwerksicherheit, SIEM, Threat Hunting und Offensive Security lagen. Weniger stark nachgefragt wurden hingegen Themen wie ICS-Sicherheit oder Cyberkriegsführung. Im Hinblick auf die als relevant wahrgenommenen Bedrohungen wurden insbesondere Ransomware, Phishing, Malware und Cyber-Spionage hervorgehoben. Diese Ergebnisse liefern wichtige Hinweise für die Priorisierung zukünftiger Ausbildungsinhalte und bestätigen, dass insbesondere praxisnahe, angriffsbezogene und unmittelbar anwendbare Themenfelder für die Zielgruppe von hoher Relevanz sind. Zugleich zeigen sie, dass die Wahrnehmung der Bedrohungslage stark von jenen Angriffsformen geprägt ist, die im öffentlichen und operativen Diskurs besonders präsent sind. Bezüglich des Wissensstands wurde deutlich, dass grundlegende Konzepte wie die CIA-Triad vielen Teilnehmenden bereits bekannt waren. Gleichzeitig zeigten sich deutliche Wissenslücken in Bezug auf Standards, Normen und Frameworks wie COBIT, ITIL, IEC 62443 oder die CIS Controls. Daraus ergibt sich ein klarer curricularer Bedarf, grundlegende Frameworks und Standards zumindest in einführender Form in das Ausbildungsprogramm aufzunehmen. Der Befund legt nahe, dass das zukünftige Curriculum nicht nur technisch-instrumentelle Kompetenzen adressieren sollte, sondern auch ein Orientierungswissen über relevante Referenzrahmen und etablierte Ordnungssysteme des Cybersecurity-Bereichs vermitteln muss.

Auch die praktische Übungsphase lieferte wichtige Hinweise auf bestehende Ausbildungsbedarfe. So zeigte sich, dass Vorkenntnisse im Bereich SIEM und Linux innerhalb der Zielgruppe nur eingeschränkt vorhanden waren. Da keine der teilnehmenden Personen zuvor mit einem SIEM-System gearbeitet hatte, wurde der Schwierigkeitsgrad der Übung von sämtlichen Teilnehmenden als hoch oder sehr hoch eingeschätzt. Diese Rückmeldung ist in mehrfacher Hinsicht aufschlussreich. Einerseits bestätigt sie die Relevanz entsprechender technischer Grundlagen für praxisnahe Ausbildungsformate. Andererseits macht sie deutlich, dass zukünftige praktische Einheiten einer vorgelagerten Einführung in SIEM-Technologien, Linux-Grundlagen und Analysewerkzeuge bedürfen, um Überforderung zu vermeiden und eine belastbare Ausgangsbasis für weiterführende Übungen zu schaffen. Hinsichtlich der didaktischen Gestaltung sprach sich die Zielgruppe deutlich für praxisorientierte Lern- und Prüfungsformate aus. Besonders positiv bewertet wurden Übungen mit konkretem Anwendungsbezug; auch die eingesetzten Angriffsszenarien wurden insgesamt als relevant und motivierend eingeschätzt. Zudem zeigte sich eine hohe Bereitschaft, Cyberübungen als festen Bestandteil der Ausbildung zu akzeptieren. Als zentrale Anforderungen an Trainerinnen und Trainer nannten die Teilnehmenden insbesondere hohe Fachkompetenz, nachgewiesene Praxiserfahrung, Geduld sowie die Fähigkeit, konstruktives Feedback zu geben. Im qualitativen Feedback wurde darüber hinaus der Wunsch nach stärkerer theoretischer Vorbereitung und einem strukturierteren Onboarding vor praktischen Übungen geäußert. Daraus folgt die Notwendigkeit einer klareren didaktischen Progression, in der theoretische Grundlagen, Tool-Einführungen und praktische Anwendung systematisch aufeinander aufbauen. Insgesamt liefert der Workshop mehrere zentrale Erkenntnisse für die Bedarfsanalyse des Projekts Bumblebee. Erstens bestätigt sich die Notwendigkeit eines gestuften

Ausbildungskonzepts, das unterschiedliche Vorkenntnisse innerhalb der Zielgruppe berücksichtigt. Zweitens zeigt sich ein klarer Bedarf an praxisorientierten Ausbildungsformaten mit realistischen Angriffsszenarien und konkreten Handlungsabläufen. Drittens müssen grundlegende Kenntnisse in SIEM, Linux sowie in ausgewählten Normen und Frameworks curricular berücksichtigt werden, um die Teilnehmenden angemessen auf praktische Übungen vorzubereiten. Der Workshop stellt damit eine wesentliche empirische Grundlage für die weitere Ausgestaltung des Curriculums dar und verbindet Erkenntnisse zu fachlichen Bedarfen der Zielgruppe mit zentralen didaktischen Anforderungen zukünftiger Ausbildungs- und Übungsformate.

3.4.4 Workshop 19.02.2024

Der Workshop vom 19. Februar 2024 hatte das Ziel, weitere Anforderungen an ein zukünftiges Ausbildungsprogramm im Bereich Cybersicherheit aus der Perspektive militärischer Ausbilder zu erheben. Im Zentrum standen dabei insbesondere die Reflexion bestehender Ausbildungsprogramme, die Analyse organisatorischer Rahmenbedingungen innerhalb des Bundesheeres sowie die Präzisierung jener inhaltlichen, strukturellen und didaktischen Anforderungen, die ein zukünftiger Cybersecurity-Kurs erfüllen sollte. Der Workshop knüpfte damit an die zuvor gewonnenen Erkenntnisse an und verfolgte das Ziel, diese aus Sicht jener Akteursgruppe zu vertiefen, die mit der praktischen Vermittlung technischer und organisationsbezogener Inhalte betraut ist.

Aus wissenschaftlicher Perspektive ist diesem Workshop eine besondere Bedeutung beizumessen, da die Perspektive der Ausbilder eine zentrale Vermittlungsinstanz zwischen institutionellen Anforderungen, didaktischer Umsetzbarkeit und realer Zielgruppenorientierung darstellt. Die im Rahmen des Workshops gewonnenen Erkenntnisse tragen daher nicht nur zur inhaltlichen Präzisierung des Ausbildungsbedarfs bei, sondern erlauben auch Rückschlüsse darauf, welche strukturellen Voraussetzungen, methodischen Zugänge und curricularen Schwerpunktsetzungen aus Sicht der Ausbildungspraxis als realistisch und zielführend eingeschätzt werden.

3.4.5 Aktuelle Ausbildungsstruktur

Zu Beginn des Workshops wurde die aktuelle Ausbildungssituation im Bereich der Informations- und Kommunikationstechnologie innerhalb des Bundesheeres analysiert. Dabei zeigte sich, dass bereits mehrere Ausbildungswege existieren, die technische Grundlagen vermitteln, jedoch nur in begrenztem Umfang spezifische Inhalte der Cybersicherheit abdecken. Zu den bestehenden Ausbildungsangeboten zählen insbesondere der Bachelorstudiengang Militärische Informations- und Kommunikationstechnologie an der Militärakademie, verschiedene technische Studienprogramme im zivilen Bereich, etwa im Umfeld von IT-Infrastrukturmanagement oder IT-Security, sowie einzelne Lehrveranstaltungen zu Themen wie sichere Informationssysteme oder Security Information Management. Diese Vielfalt an Ausbildungswegen verweist auf ein grundsätzlich vorhandenes institutionelles Fundament, macht jedoch zugleich deutlich, dass die Cybersicherheitsausbildung bislang nur teilweise systematisch und eigenständig ausdifferenziert ist.

Von besonderer Bedeutung ist in diesem Zusammenhang der Befund, dass derzeit kein vollständiger Masterstudiengang im Bereich Cybersecurity innerhalb des Bundesheeres existiert. Offiziere, die eine weiterführende Spezialisierung auf Master-Niveau anstreben, müssen entsprechende Studiengänge daher gegenwärtig an zivilen Universitäten absolvieren. Zwar wird der Bachelorabschluss der Militärakademie grundsätzlich als Zugangsvoraussetzung für weiterführende Masterstudien anerkannt, dennoch verweist diese Situation auf eine institutionelle Lücke in der vertieften militärischen Cyberausbildung. Damit verbunden ist die Herausforderung, dass höher qualifiziertes Personal im Bereich der Cybersicherheit in besonderem Maße am



externen Arbeitsmarkt nachgefragt wird. Im Workshop wurde dementsprechend darauf hingewiesen, dass viele Absolventinnen und Absolventen nach Abschluss ihrer Ausbildung in die Privatwirtschaft wechseln, wodurch dem Bundesheer ein Teil der ausgebildeten Fachkräfte langfristig nicht erhalten bleibt. Dieser Befund ist für die Bedarfserhebung insofern relevant, als ein zukünftiges Ausbildungsprogramm nicht nur fachlich angemessen gestaltet sein muss, sondern auch innerhalb eines institutionellen Umfelds verortet ist, das durch Fachkräftemobilität und Konkurrenz um qualifiziertes Personal geprägt ist.

Ergänzend wurde darauf verwiesen, dass an der Führungsunterstützungsschule bestimmte Inhalte der Militärakademie in verkürzter Form vermittelt werden sollen. Dies deutet darauf hin, dass bereits Ansätze einer gestuften oder differenzierten Wissensvermittlung vorhanden sind, allerdings noch nicht in Form eines klar konsolidierten, auf Cybersicherheit ausgerichteten Gesamtkonzepts. Insgesamt zeigt die Analyse der aktuellen Ausbildungsstruktur damit, dass zwar einzelne Ausbildungsbausteine und institutionelle Anknüpfungspunkte bestehen, ein kohärentes, explizit auf operative Cybersicherheitskompetenz ausgerichtetes Ausbildungsprogramm jedoch bislang nur in Ansätzen vorhanden ist. Daraus ergibt sich ein deutliches Argument für die Entwicklung eines eigenständigen, curricular strukturierten Ausbildungsangebots.

3.5 Identifizierte Herausforderungen und Entwicklungsbedarfe

Die Darstellung der aktuellen Ausbildungsstruktur bildet die notwendige Grundlage, um bestehende Stärken, Begrenzungen und Entwicklungsbedarfe systematisch einzuordnen. Für die Konzeption eines zielgerichteten Ausbildungsprogramms ist es nicht ausreichend, die gegenwärtigen organisatorischen und inhaltlichen Gegebenheiten lediglich deskriptiv zu erfassen; vielmehr ist zu analysieren, in welchen Bereichen bestehende Strukturen den aktuellen und absehbaren Anforderungen des militärischen Cyberkontexts bereits entsprechen und wo strukturelle, inhaltliche oder didaktische Anpassungen erforderlich sind. Vor diesem Hintergrund werden im folgenden Abschnitt jene Herausforderungen und Entwicklungsbedarfe herausgearbeitet, die sich aus der gegenwärtigen Ausbildungsrealität ergeben. Im Fokus stehen dabei insbesondere Fragen der inhaltlichen Aktualität, der didaktischen Anschlussfähigkeit, der organisatorischen Umsetzbarkeit sowie der Ausrichtung auf die spezifischen Kompetenzanforderungen eines SOC-/NOC-nahen Einsatzumfelds. Die Analyse dient damit als Brücke zwischen der Bestandsaufnahme der bestehenden Ausbildungsstruktur und der nachfolgenden Ableitung konkreter Anforderungen an das Curriculum.

3.5.1 Anforderungen an das Curriculum

Im Rahmen des Workshops wurde deutlich betont, dass das geplante Ausbildungsprogramm bewusst auf einem grundlegenden operativen Kompetenzniveau ansetzen sollte. Ziel ist nicht die Ausbildung hochspezialisierter Cybersecurity-Expertinnen und -Experten, sondern die Befähigung von Personal, operative Aufgaben im Bereich der Überwachung, Erkennung und ersten Analyse von IT-bezogenen Sicherheitsvorfällen sachgerecht wahrzunehmen. Diese Schwerpunktsetzung ist für die curriculare Konzeption von zentraler Bedeutung, da sie den Ausbildungsanspruch klar von spezialisierten Fachdisziplinen wie digitaler Forensik, Softwareentwicklung oder fortgeschrittener technischer Analyse abgrenzt. Der zukünftige Kurs soll demnach ein Qualifikationsprofil adressieren, das auf Handlungssicherheit im Erstreaktions- und Überwachungskontext ausgerichtet ist.

Die Absolventinnen und Absolventen eines solchen Ausbildungsformats sollen insbesondere dazu befähigt werden, definierte Prozesse im Falle eines Cybervorfalls korrekt abzuarbeiten, sicherheitsrelevante Ereignisse zu erkennen, grundlegende Firewall-Regeln zu verstehen und anzuwenden, Auffälligkeiten in System- und Netzwerkprotokollen zu identifizieren sowie Incident-Response-Prozesse einzuleiten. Die Zielsetzung des Curriculums liegt somit in der Entwicklung eines operativ verwendbaren Grundverständnisses, das technische Beobachtungskompetenz mit prozessualer Handlungssicherheit verbindet. Dabei wurde im Workshop ausdrücklich hervorgehoben, dass tiefergehende Aufgaben wie digitale Forensik, Systementwicklung oder Programmierung nicht Teil des Ausbildungsziels sein sollen. Die Teilnehmenden sollen im späteren Einsatz mit bestehenden Systemen arbeiten, diese überwachen und auf erkennbare Auffälligkeiten angemessen reagieren können. Daraus ergibt sich ein klares curriculares Leitbild, das sich an der Rolle des technisch handlungsfähigen Erstreaktionspersonals orientiert.

Inhaltlich wurden mehrere Themenbereiche als besonders relevant für das Curriculum identifiziert. Dazu zählen OSINT und Social Engineering, Angreiferverhalten und Angriffsmethoden, Grundlagen der Kryptografie, System- und Netzwerktests, Information and Asset Classification, die Configuration Management Database, SIEM-Systeme und Log-Analyse sowie Incident Response. Diese Themenfelder bilden zusammen ein Kompetenzspektrum, das sowohl technische Grundlagen als auch organisations- und prozessorientierte Inhalte umfasst. Von besonderer Relevanz ist dabei die Log-Analyse, da Teilnehmende lernen sollen, zwischen regulären Systemereignissen und tatsächlich sicherheitsrelevanten Vorfällen zu unterscheiden. Gerade diese Unterscheidungsfähigkeit ist für operative Erstreaktionsrollen zentral, da sie die Grundlage

für angemessene Eskalations- und Reaktionsentscheidungen bildet. Komplexere Themen wie Data Analytics oder vertiefte digitale Forensik wurden hingegen als für die unmittelbare Zielgruppe weniger relevant bewertet. Dieser Befund unterstreicht erneut, dass das Ausbildungsprogramm nicht auf Spezialisierung, sondern auf handlungspraktische Basiskompetenz ausgerichtet sein sollte.

3.5.2 Organisation und Rahmenbedingungen der Ausbildung

Neben den inhaltlichen Anforderungen wurden im Workshop auch organisatorische und strukturelle Rahmenbedingungen der Ausbildung ausführlich diskutiert. Diese Aspekte sind für die spätere Curriculumsentwicklung insofern von hoher Bedeutung, als die Qualität und Wirksamkeit eines Ausbildungsprogramms nicht nur von den vermittelten Inhalten, sondern ebenso von seiner organisatorischen Einbettung, der Lehrform und den institutionellen Umsetzungsbedingungen abhängen. Hinsichtlich der Kursdauer wurde eine Mindestdauer von zwei Wochen als erforderlich betrachtet, während zwei bis drei Wochen als realistischer Gesamtrahmen für ein grundlegendes Ausbildungsprogramm eingeschätzt wurden. Eine Dauer von drei Wochen wurde dabei als obere Grenze angesehen. Diese Einschätzung korrespondiert mit den Ergebnissen der vorangegangenen Workshops und verweist darauf, dass das angestrebte Kompetenzprofil in einem kompakten, aber ausreichend strukturierten Ausbildungsformat vermittelt werden kann, sofern die inhaltliche Auswahl klar priorisiert wird.

Als fachliche Eingangsvoraussetzung wurde der bereits bestehende IKT-Grundlagenkurs des Bundesheeres genannt, der etwa eine Woche dauert. Dieser Kurs kann als Vorstufe oder Basisqualifikation für das geplante Ausbildungsprogramm verstanden werden. Daraus ergibt sich die Möglichkeit, das zukünftige Curriculum auf bereits vorhandene technische Grundkenntnisse aufzubauen, ohne den Kurs selbst mit zu vielen elementaren Vorinhalten zu überladen. Zugleich eröffnet dies die Perspektive einer gestuften Ausbildungslogik, in der Grundlagen- und Vertiefungsformate stärker aufeinander abgestimmt werden. Auch die Gruppengröße wurde differenziert betrachtet. Als optimale Teilnehmerzahl wurden etwa zehn Personen genannt, während für Theorieeinheiten eine Obergrenze von rund zwanzig Personen und für praktische Übungen eine maximale Gruppengröße von etwa sechzehn Personen als vertretbar erachtet wurde. Diese Einschätzungen machen deutlich, dass insbesondere die praktische Ausbildung auf intensive Betreuung, unmittelbares Feedback und eine überschaubare Gruppendynamik angewiesen ist. Für die spätere Ausgestaltung des Ausbildungsprogramms bedeutet dies, dass organisatorische Skalierbarkeit nicht zulasten didaktischer Qualität gehen darf.

Bezüglich der Lehrform bestand Einigkeit darüber, dass die Ausbildung grundsätzlich in Präsenz stattfinden sollte. Digitale Lernplattformen wie Moodle wurden zwar als sinnvolle Ergänzung zum Austausch von Lernmaterialien, zur Bereitstellung von Unterlagen oder zur organisatorischen Unterstützung betrachtet, jedoch nicht als primäre Lehrplattform empfohlen. Dieser Befund deutet darauf hin, dass die Vermittlung operativer Cybersicherheitskompetenz in diesem Kontext stark auf unmittelbare Interaktion, Anleitung und praktische Übungsanteile angewiesen ist. Ergänzend wurde angemerkt, dass Lehrpersonal innerhalb des Bundesheeres verpflichtende pädagogische und didaktische Ausbildungen absolvieren muss. Dieser Umstand verweist darauf, dass auch auf Seiten der Lehrenden institutionelle Qualitätsanforderungen bestehen, die für die Umsetzung eines künftigen Ausbildungsprogramms genutzt und weiterentwickelt werden können.

3.5.3 Prüfungen und Evaluierung

Ein weiterer Themenbereich des Workshops betraf die Frage, wie Lehrinhalte überprüft und die Qualität des Ausbildungsprogramms langfristig gesichert werden können. Dabei wurde deutlich, dass eine angemessene Leistungsfeststellung sowohl schriftliche Prüfungsformate als auch praktische Übungen umfassen sollte. Diese Kombination erscheint aus didaktischer Sicht

plausibel, da sie einerseits die Überprüfung konzeptionellen und prozessualen Wissens ermöglicht und andererseits handlungsbezogene Kompetenzen sichtbar macht, die sich in reinen Wissenstests nur unzureichend abbilden lassen. Gerade im Bereich der Cybersicherheitsausbildung, in dem operative Handlungssicherheit und situative Entscheidungsfähigkeit von besonderer Bedeutung sind, erscheint eine mehrdimensionale Prüfungslogik besonders sinnvoll. Darüber hinaus wurde vorgeschlagen, zu Beginn einzelner Module kurze Eingangsüberprüfungen durchzuführen, um bereits vorhandene Kenntnisse der Teilnehmenden besser einschätzen zu können. Ein solches Vorgehen kann didaktisch dazu beitragen, Ausbildungsinhalte differenzierter auf den Wissensstand der Zielgruppe abzustimmen und gegebenenfalls notwendige Vorkenntnisse zu aktivieren oder auszugleichen. Für einzelne Module wurde zudem angeregt, Abschlussprüfungen unmittelbar nach Beendigung der jeweiligen Unterrichtseinheit durchzuführen. Dabei wurde betont, dass den Teilnehmenden ausreichend Zeit für die Vorbereitung auf diese Prüfungen eingeräumt werden sollte. Dieser Hinweis verweist auf die Notwendigkeit, Prüfungsformate nicht nur als Kontrollinstrumente, sondern als integralen Bestandteil eines lernförderlichen Ausbildungsdesigns zu verstehen.

Neben der Leistungsüberprüfung der Teilnehmenden wurde auch die regelmäßige Evaluierung und Aktualisierung der Ausbildungsunterlagen thematisiert. Als sinnvoller Richtwert wurde eine Überprüfung im Abstand von zwei bis fünf Jahren genannt. Angesichts der hohen Dynamik des Cyberbereichs ist diese Einschätzung besonders relevant, da technische Entwicklungen, Bedrohungsmuster und organisatorische Anforderungen einem kontinuierlichen Wandel unterliegen. Die systematische Aktualisierung der Lehrmaterialien ist daher nicht als optionaler Zusatz, sondern als notwendige Voraussetzung für die langfristige Relevanz und Qualität des Ausbildungsprogramms zu betrachten.

3.5.4 Relevanz aktueller Cyberbedrohungen

Im Rahmen des Workshops wurde darüber hinaus eine differenzierte Einschätzung der Relevanz verschiedener Cyberbedrohungen für den militärischen Ausbildungskontext vorgenommen. Ziel dieser Einordnung war es, jene Bedrohungstypen zu identifizieren, die für die angestrebte Zielgruppe nicht nur aus sicherheitsbezogener Sicht bedeutsam, sondern auch im Hinblick auf ihre operative Anschlussfähigkeit, ihre didaktische Vermittelbarkeit und ihre praktische Relevanz innerhalb eines grundlegenden Ausbildungsprogramms besonders geeignet erscheinen. Als besonders relevant wurden dabei insbesondere Phishing, Malware, Ransomware, Denial-of-Service-Angriffe sowie die Manipulation von Informationen und Daten eingestuft. Diese Auswahl verweist auf Bedrohungsformen, die im gegenwärtigen Cyberraum sowohl eine hohe praktische Eintrittswahrscheinlichkeit als auch eine unmittelbare Relevanz für operative Erstreaktions- und Überwachungsaufgaben besitzen. Zugleich handelt es sich um Angriffsmuster, die in ihrer Grundlogik hinreichend konkret, beobachtbar und in realitätsnahen Trainingsszenarien abbildbar sind, sodass sie sich in besonderer Weise für die Vermittlung anwendungsorientierter Handlungskompetenzen eignen.

Die Hervorhebung dieser Bedrohungstypen ist auch deshalb bedeutsam, weil sie typische Situationen repräsentieren, mit denen Personal in SOC-/NOC-nahen Funktionen im Rahmen der Erstwahrnehmung, Voranalyse und Weiterleitung sicherheitsrelevanter Ereignisse konfrontiert sein kann. Phishing-Angriffe etwa erfordern die Fähigkeit, verdächtige Kommunikationsmuster zu erkennen, Indikatoren für Täuschungsversuche zu identifizieren und potenzielle Auswirkungen auf Benutzerkonten, Systeme oder Kommunikationsabläufe einzuschätzen. Malware- und Ransomware-Vorfälle verlangen darüber hinaus ein grundlegendes Verständnis möglicher Infektionspfade, Ausbreitungsmechanismen und erster Eindämmungsmaßnahmen, ohne dabei bereits tiefgehende forensische Spezialkompetenzen vorauszusetzen. Denial-of-Service-Angriffe und die Manipulation von Informationen oder Daten verweisen wiederum auf Szenarien, in denen

Verfügbarkeit, Integrität und Vertrauenswürdigkeit informationstechnischer Systeme unmittelbar betroffen sind. Für die Ausbildung bedeutet dies, dass Teilnehmende lernen müssen, solche Vorfälle nicht nur technisch zu erkennen, sondern sie auch hinsichtlich ihrer operativen Tragweite, ihrer Dringlichkeit und ihrer prozessualen Weiterverarbeitung einzuordnen. Aus didaktischer Perspektive ist die Konzentration auf diese Bedrohungstypen ebenfalls plausibel, da sie eine Verbindung zwischen technischer Ereigniserkennung, organisatorischer Reaktion und kommunikativer Eskalation ermöglichen. Sie bieten damit einen geeigneten Ausgangspunkt, um jene Kompetenzen zu fördern, die für ein grundlegendes militärisches Ausbildungsprogramm im Bereich Cybersicherheit zentral sind: die strukturierte Wahrnehmung auffälliger Ereignisse, die Unterscheidung zwischen regulären und sicherheitsrelevanten Vorkommnissen, die nachvollziehbare Dokumentation von Beobachtungen sowie die regelgeleitete Weitergabe an zuständige Stellen. Die Auswahl relevanter Bedrohungen ist daher nicht nur Ausdruck einer inhaltlichen Priorisierung, sondern zugleich ein wesentlicher Bestandteil der curriculären Fokussierung auf operativ anschlussfähige Erstreaktionskompetenz.

Demgegenüber wurden andere Bedrohungsformen wie hybride Kriegsführung, Deepfakes oder Angriffe auf Waffensysteme im Hinblick auf die unmittelbare Zielgruppe als weniger relevant bewertet. Diese Einschätzung ist jedoch nicht dahingehend zu verstehen, dass solche Phänomene im sicherheitspolitischen oder militärstrategischen Gesamtbild vernachlässigbar wären. Vielmehr verweist sie auf die Notwendigkeit, zwischen der allgemeinen sicherheitspolitischen Bedeutung bestimmter Bedrohungen und ihrer konkreten Eignung als Ausbildungsgegenstand für eine bestimmte Zielgruppe zu unterscheiden. Hybride Kriegsführung etwa stellt ein komplexes, multidimensionales Phänomen dar, das politische, kommunikative, technologische und gesellschaftliche Einflussdimensionen umfasst und daher eher einer strategischen oder interdisziplinären Betrachtung bedarf als einer primär operativen Grundlagenausbildung. Ähnliches gilt für Deepfake-Technologien oder Angriffe auf Waffensysteme, die teilweise spezialisierte technische, rechtliche oder nachrichtendienstliche Kenntnisse voraussetzen und damit nur bedingt in ein grundlegendes Ausbildungsformat für SOC-/NOC-nahe Rollen integrierbar sind.

Der Workshop verdeutlicht damit, dass die Relevanz von Bedrohungen nicht abstrakt oder ausschließlich auf Basis ihrer öffentlichen Sichtbarkeit bestimmt werden kann. Vielmehr ist sie stets in Relation zum angestrebten Kompetenzniveau, zur institutionellen Funktion der Zielgruppe und zu den konkreten Handlungsanforderungen des späteren Einsatzkontexts zu bewerten. Für die curriculare Planung besitzt diese Einsicht erhebliche Bedeutung, da sie eine gezielte Schwerpunktsetzung auf jene Angriffstypen ermöglicht, die für die Ausbildung operativer Erstreaktionskompetenz den höchsten Mehrwert versprechen. Eine solche Fokussierung trägt nicht nur zur inhaltlichen Klarheit des Curriculums bei, sondern erhöht auch dessen didaktische Wirksamkeit, da die vermittelten Inhalte enger an realistischen Handlungssituationen, beobachtbaren Bedrohungsmustern und tatsächlich relevanten Reaktionsprozessen ausgerichtet werden können. In diesem Sinne bildet die Priorisierung bestimmter Bedrohungstypen einen wesentlichen Schritt zur Entwicklung eines Ausbildungsprogramms, das sowohl praxisnah als auch funktional auf die Anforderungen des militärischen Cyberkontexts abgestimmt ist.

3.5.5 Relevante Standards und Rahmenwerke

Zusätzlich wurde im Rahmen des Workshops diskutiert, welche internationalen Standards und Rahmenwerke bei der Konzeption und inhaltlichen Ausgestaltung des Ausbildungsprogramms berücksichtigt werden sollten. Ziel dieser Diskussion war es, jene Referenzmodelle zu identifizieren, die sich in besonderer Weise dazu eignen, die fachlichen Inhalte des Programms zu strukturieren, organisatorische und prozessuale Anforderungen nachvollziehbar abzubilden und zugleich eine Anschlussfähigkeit an etablierte sicherheitsbezogene Praktiken und militärische Rahmenbedingungen herzustellen. Als besonders relevant wurden in diesem Zusammenhang

ISO/IEC 27001, ITIL, das NIST Cybersecurity Framework sowie STANAG-Dokumente genannt. Diese Auswahl ist insofern aufschlussreich, als sie unterschiedliche, jedoch komplementäre Perspektiven auf Cybersicherheit und Sicherheitsmanagement vereint. Während ISO/IEC 27001 vor allem einen normativen Bezugsrahmen für Informationssicherheitsmanagement bereitstellt, verweist ITIL auf die Bedeutung strukturierter Service- und Prozesslogiken. Das NIST Cybersecurity Framework bietet darüber hinaus eine breit anwendbare Systematik zur Einordnung sicherheitsrelevanter Maßnahmen entlang zentraler Handlungsfelder, während STANAG-Dokumente einen spezifisch militärischen Bezugsrahmen darstellen, der die institutionelle Anschlussfähigkeit im Verteidigungskontext unterstützt. Die Relevanz dieser Referenzrahmen liegt nicht allein in ihrer fachlichen Bekanntheit oder internationalen Verbreitung, sondern insbesondere darin, dass sie unterschiedliche Dimensionen des angestrebten Ausbildungsprofils adressieren. Sie ermöglichen es, technische Inhalte nicht isoliert zu vermitteln, sondern in übergeordnete organisatorische, prozessuale und institutionelle Zusammenhänge einzubetten. Für ein militärisch ausgerichtetes Ausbildungsprogramm ist dies von besonderer Bedeutung, da operative Handlungssicherheit im Cyberbereich nicht nur auf technischem Wissen beruht, sondern ebenso auf dem Verständnis standardisierter Abläufe, definierter Rollen, geregelter Meldewege und nachvollziehbarer Sicherheitsprozesse. Die Einbindung solcher Standards und Rahmenwerke kann daher dazu beitragen, das Ausbildungsprogramm konzeptionell zu stabilisieren und den Teilnehmenden Orientierungswissen zu vermitteln, das über die Bearbeitung einzelner technischer Vorfälle hinausweist.

Aus curricularer Perspektive folgt daraus, dass Standards und Rahmenwerke nicht lediglich als theoretische Hintergrundinformation behandelt werden sollten. Vielmehr können sie als strukturierende Elemente dienen, um den Teilnehmenden ein grundlegendes Verständnis dafür zu vermitteln, wie sicherheitsrelevante Maßnahmen in formalisierte Prozesse, institutionelle Verantwortlichkeiten und organisationsbezogene Steuerungslogiken eingebettet sind. Die Auseinandersetzung mit solchen Modellen kann damit einen wichtigen Beitrag dazu leisten, technische Beobachtungen, organisatorische Abläufe und reaktive Maßnahmen in einen größeren konzeptionellen Zusammenhang einzuordnen. Dies ist insbesondere für Zielgruppen relevant, die später nicht primär spezialisierte Expertentätigkeiten ausüben, sondern in operativen Kontexten auf Basis definierter Prozesse handeln und Entscheidungen vorbereiten oder weiterleiten sollen.

Im Workshop wurden darüber hinaus auch weitere Standards und Rahmenwerke wie COBIT, IEC 62443 oder die CIS Controls erwähnt. Diese wurden jedoch im Hinblick auf die unmittelbare Zielgruppe als weniger zentral eingeschätzt. Auch dieser Befund verweist auf eine klare Priorisierungslogik innerhalb der Curriculumsentwicklung. Nicht sämtliche im Bereich der Cybersicherheit etablierten Standards müssen in gleichem Umfang Bestandteil eines grundlegenden Ausbildungsprogramms sein. Vielmehr ist eine differenzierte Auswahl erforderlich, die sich an der operativen Relevanz, am angestrebten Kompetenzniveau sowie an der Funktion des konkreten Ausbildungsformats orientiert. Während etwa COBIT stärker governance- und steuerungsbezogene Perspektiven adressiert und IEC 62443 vor allem im industriellen beziehungsweise OT-nahen Kontext besondere Relevanz entfaltet, erscheinen diese Rahmenwerke für eine grundlegende Ausbildung von Personal in SOC-/NOC-nahen Rollen nur bedingt prioritär. Ähnliches gilt für die CIS Controls, die zwar praxisnahe Orientierung bieten, jedoch im Rahmen eines einführenden Ausbildungsprogramms nicht notwendigerweise denselben Stellenwert besitzen wie stärker prozess- und managementbezogene Referenzmodelle.

Die Diskussion im Workshop macht damit deutlich, dass die Auswahl geeigneter Standards und Rahmenwerke nicht nach dem Prinzip größtmöglicher Vollständigkeit erfolgen sollte, sondern entlang didaktischer und funktionaler Gesichtspunkte. Für die Curriculumsentwicklung bedeutet dies, dass jene Referenzmodelle bevorzugt berücksichtigt werden sollten, die einerseits ein grundlegendes Verständnis sicherheitsrelevanter Prozesse fördern und andererseits eine

unmittelbare Anschlussfähigkeit an den institutionellen und operativen Kontext des Bundesheeres aufweisen. Standards und Frameworks sind in diesem Sinne nicht als additive Zusatzinhalte zu verstehen, sondern als konzeptionelle Bezugspunkte, die dazu beitragen, fachliche Inhalte zu strukturieren, Rollenverständnisse zu schärfen und die spätere Anwendung sicherheitsbezogener Maßnahmen in institutionell geregelte Abläufe einzuordnen. Ihre curriculare Funktion besteht folglich nicht in der vollständigen Vermittlung normativer Detailtiefe, sondern in der Herstellung eines Orientierungswissens, das den Teilnehmenden hilft, technische, organisatorische und sicherheitsbezogene Fragestellungen in einem größeren systematischen Zusammenhang zu verstehen.

3.5.6 Einordnung der Ergebnisse des Workshops

Insgesamt zeigt der Workshop vom 19. Februar 2024, dass sich die organisatorischen, curricularen und institutionellen Rahmenbedingungen der militärischen Cybersicherheitsausbildung gegenwärtig noch in einem Entwicklungs- und Konsolidierungsprozess befinden. Dieser Befund verweist darauf, dass zwar bereits einzelne Ausbildungsbausteine, thematische Anknüpfungspunkte und institutionelle Zuständigkeiten vorhanden sind, ein in sich geschlossenes, systematisch aufgebautes und auf die spezifischen Anforderungen des militärischen Cyberkontexts ausgerichtetes Ausbildungskonzept jedoch bislang nur in Ansätzen vorliegt. Gerade vor diesem Hintergrund kommt den im Workshop gewonnenen Erkenntnissen besondere Bedeutung zu, da sie dazu beitragen, bestehende Strukturen nicht nur deskriptiv zu erfassen, sondern im Hinblick auf ihren Weiterentwicklungsbedarf analytisch einzuordnen. Zugleich konnten im Rahmen des Workshops zentrale Anforderungen an die Struktur, die inhaltliche Ausrichtung, die Lehrform, die Prüfungslogik sowie die institutionelle Einbettung eines zukünftigen Ausbildungsprogramms identifiziert werden. Die Ergebnisse machen deutlich, dass ein solches Programm weder als rein technisches Schulungsformat noch als abstrakt-theoretische Vermittlung sicherheitsbezogenen Wissens konzipiert werden sollte. Vielmehr bedarf es eines Ausbildungsansatzes, der technische Grundkompetenzen, organisatorische Prozesskenntnisse und didaktisch sinnvoll aufgebaute Lernformate in einer Weise miteinander verbindet, die den realen Handlungsanforderungen der Zielgruppe entspricht. Der Workshop verdeutlicht damit, dass die Entwicklung eines tragfähigen Curriculums nicht allein von der Auswahl relevanter Inhalte abhängt, sondern in gleichem Maße von der Frage, in welcher Form diese Inhalte vermittelt, überprüft und in bestehende Ausbildungsstrukturen integriert werden können.

Besonders deutlich wird in diesem Zusammenhang, dass das zukünftige Ausbildungsprogramm auf einem grundlegenden operativen Kompetenzniveau ansetzen sollte. Im Zentrum steht demnach nicht die Ausbildung hochspezialisierter Fachkräfte für vertiefte Analysen oder hochkomplexe technische Spezialdisziplinen, sondern die Befähigung von Personal zur Wahrnehmung klar umrissener Erstreaktions-, Überwachungs- und Unterstützungsaufgaben im SOC-/NOC-nahen Umfeld. Daraus folgt eine curriculare Schwerpunktsetzung, die sich an realistischen Einsatz- und Reaktionsanforderungen orientiert und insbesondere jene Kompetenzen adressiert, die für die Erkennung, erste Einordnung, strukturierte Dokumentation und regelgeleitete Eskalation sicherheitsrelevanter Ereignisse erforderlich sind. Ein solches Kompetenzprofil ist im militärischen Kontext von besonderer Relevanz, da operative Handlungsfähigkeit hier nicht allein durch technisches Wissen, sondern durch dessen verlässliche Einbettung in institutionelle Abläufe, Kommunikationsstrukturen und Verantwortungszusammenhänge bestimmt wird.

Die Ergebnisse des Workshops unterstreichen darüber hinaus, dass ein wirksames Ausbildungsprogramm sowohl technische als auch organisatorische Handlungssicherheit fördern muss. Technische Inhalte wie Log-Analyse, Firewall-Grundlagen, Angriffserkennung oder der Umgang mit Monitoring- und Incident-Response-Prozessen entfalten ihren praktischen Wert erst dann in vollem Umfang, wenn sie mit einem Verständnis für Meldewege, Rollenverteilungen,

Eskalationslogiken und institutionelle Zuständigkeiten verbunden werden. Der Workshop bestätigt damit eine zentrale Annahme der vorliegenden Bedarfsanalyse: Cybersicherheitsausbildung im militärischen Kontext kann nicht auf technische Fertigkeiten reduziert werden, sondern muss als integrierter Qualifizierungsprozess verstanden werden, der technische, organisatorische und didaktische Dimensionen systematisch miteinander verschränkt. Insgesamt leistet der Workshop damit einen wesentlichen Beitrag zur Präzisierung jener Anforderungen, die für die Entwicklung eines praktisch anschlussfähigen und institutionell tragfähigen Ausbildungsformats im Projekt Bumblebee maßgeblich sind. Sein Erkenntniswert liegt nicht nur in der Benennung einzelner Ausbildungsinhalte oder organisatorischer Rahmenbedingungen, sondern vor allem in der verdichteten Herausarbeitung eines handlungsorientierten Anforderungsprofils, das als Brücke zwischen institutioneller Realität, operativem Bedarf und curricularem Entwicklungsanspruch fungiert. Der Workshop stellt damit einen zentralen Baustein innerhalb der empirischen Bedarfserhebung dar und trägt wesentlich dazu bei, die Grundlage für ein Ausbildungskonzept zu schaffen, das sowohl den Anforderungen der Zielgruppe als auch den strukturellen Bedingungen des militärischen Umfelds gerecht wird.

3.5.7 Synthese der Bedarfserhebung

Über alle durchgeführten Erhebungsformate hinweg ergibt sich ein konsistentes, in sich schlüssiges und empirisch gut abgestütztes Bedarfsprofil für die Entwicklung des geplanten Ausbildungsprogramms. Trotz unterschiedlicher Perspektiven der einbezogenen Akteursgruppen sowie der variierenden Erhebungssettings zeigen die Ergebnisse eine hohe Konvergenz hinsichtlich jener Kompetenzen, die für ein militärisch anschlussfähiges Ausbildungsformat im Bereich der Cybersicherheit als prioritär angesehen werden können. Deutlich wird insbesondere, dass das zukünftige Ausbildungsprogramm auf einem grundlegenden operativen Kompetenzniveau ansetzen sollte, das weder auf hochspezialisierte Fachqualifikationen noch auf vertiefte technische Spezialisierung abzielt, sondern auf die systematische Befähigung zur Wahrnehmung klar umrissener Erstreaktions- und Unterstützungsaufgaben in SOC-/NOC-nahen Kontexten. Damit wird ein Kompetenzprofil adressiert, das auf Handlungssicherheit im Umgang mit sicherheitsrelevanten Ereignissen ausgerichtet ist und insbesondere jene Fähigkeiten umfasst, die für die frühzeitige Erkennung, erste Einordnung und regelgeleitete Weiterverarbeitung von Vorfällen erforderlich sind. Im Zentrum des abgeleiteten Bedarfsprofils stehen folglich nicht hochkomplexe Spezialtätigkeiten wie vertiefte digitale Forensik, fortgeschrittene Malware-Analyse oder sicherheitsbezogene Systementwicklung, sondern solche Kompetenzen, die im operativen Alltag eine zuverlässige Erstbewertung und prozesssichere Reaktion ermöglichen. Hierzu zählen insbesondere die Fähigkeit zur Erkennung sicherheitsrelevanter Ereignisse, die strukturierte und nachvollziehbare Erstbewertung potenzieller Vorfälle, die sachgerechte Dokumentation relevanter Beobachtungen, die Kenntnis institutioneller Meldewege und Eskalationsmechanismen sowie die grundlegende Einordnung technischer Auffälligkeiten in Logs, Monitoring-Umgebungen und anderen sicherheitsrelevanten Systemanzeigen. Diese Anforderungen verweisen auf ein Ausbildungsverständnis, das Cybersicherheitskompetenz nicht primär als Expertenwissen, sondern als operativ nutzbare und organisationsbezogen eingebettete Handlungskompetenz konzipiert.

Zugleich zeigt die Bedarfserhebung mit besonderer Deutlichkeit, dass technische Kompetenzen allein nicht ausreichen, um den Anforderungen des militärischen Cyberkontexts gerecht zu werden. Vielmehr muss ein zukünftiges Ausbildungsprogramm so gestaltet sein, dass technische Grundlagen konsequent mit organisatorischen Abläufen, Kommunikationsanforderungen und didaktisch angemessen aufgebauten Übungs- und Anwendungsszenarien verknüpft werden. Die Ergebnisse machen deutlich, dass die Fähigkeit zur Erkennung technischer Auffälligkeiten erst dann praktisch wirksam wird, wenn sie mit einem Verständnis für Zuständigkeiten, Meldekettens, Dokumentationsanforderungen und Eskalationslogiken verbunden ist. Daraus folgt, dass die

Ausbildung nicht als isolierte Vermittlung technischer Einzelfertigkeiten verstanden werden darf, sondern als integrierter Qualifizierungsprozess, in dem technisches Wissen, prozessuale Orientierung und institutionelle Handlungssicherheit aufeinander bezogen vermittelt werden. Ein weiterer zentraler Befund der Bedarfserhebung betrifft die Heterogenität der Zielgruppe. Die unterschiedlichen Vorkenntnisse, Erfahrungsniveaus und fachlichen Hintergründe der potenziellen Teilnehmenden sprechen deutlich gegen ein didaktisch uniformes Ausbildungsmodell. Stattdessen legen die Ergebnisse ein curricular gestuftes Ausbildungskonzept nahe, das einerseits niederschwellige Zugänge für Personen mit begrenztem Vorwissen eröffnet und andererseits hinreichende Vertiefungsmöglichkeiten bietet, um praxisrelevante Kompetenzen systematisch aufzubauen. Die Notwendigkeit einer solchen gestuften Struktur ergibt sich nicht nur aus didaktischen Erwägungen, sondern auch aus dem Anspruch, ein Ausbildungsprogramm zu entwickeln, das für unterschiedliche Lerngruppen anschlussfähig bleibt, ohne den operativen Anwendungsbezug zu verlieren. Ein solcher Aufbau ermöglicht es, Grundlagenwissen, Tool-Kompetenz, Szenarienvverständnis und Reaktionslogiken schrittweise miteinander zu verknüpfen und damit eine belastbare Handlungssicherheit zu entwickeln. Die Ergebnisse sprechen zudem eindeutig für eine stark praxisorientierte Ausgestaltung des Ausbildungsprogramms. Realistische Übungsszenarien, anwendungsbezogene Aufgabenstellungen und die Arbeit mit simulationsnahen Umgebungen erscheinen als zentrale Voraussetzungen, um die angestrebten Kompetenzen nicht nur deklarativ, sondern auch handlungsbezogen zu vermitteln. Praxisorientierung ist in diesem Zusammenhang nicht als bloße Ergänzung theoretischer Inhalte zu verstehen, sondern als konstitutives Element eines wirksamen Ausbildungskonzepts. Gerade im Bereich der Cybersicherheitsausbildung, in dem Wahrnehmung, Bewertung, Dokumentation und Reaktion eng miteinander verschränkt sind, kann nachhaltige Kompetenzentwicklung nur dann gelingen, wenn die Teilnehmenden in strukturierte, realitätsnahe Handlungssituationen eingebunden werden. Dies betrifft sowohl technische Szenarien als auch kommunikative und organisatorische Anforderungen, etwa im Hinblick auf Lagebilddarstellung, Meldewege oder die koordinierte Weitergabe relevanter Informationen.

Aus den vorliegenden Befunden folgt insgesamt, dass die spätere Curriculumsentwicklung nicht primär auf Spezialisierung, sondern auf die systematische Befähigung zur sicheren, regelgeleiteten und organisationsbezogen eingebetteten Handlung im Erstreaktionskontext ausgerichtet werden sollte. Das zukünftige Ausbildungsprogramm sollte damit als grundlegendes, operativ orientiertes Qualifizierungsformat konzipiert werden, das technische, organisatorische und didaktische Anforderungen in kohärenter Weise zusammenführt. In dieser Perspektive bildet die Bedarfserhebung eine zentrale empirische Grundlage für die weitere konzeptionelle Ausarbeitung des Projekts Bumblebee. Sie liefert nicht nur Hinweise auf relevante Inhaltsbereiche, sondern formuliert zugleich die strukturellen und didaktischen Leitlinien, an denen sich die nachgelagerte Entwicklung von Lernzielen, Modularchitektur, Übungsszenarien und Evaluierungsformaten orientieren sollte.

3.6 Vergleich von Cybersicherheitsausbildung im militärischen Sektor

Die fortschreitende Digitalisierung nahezu aller gesellschaftlichen, wirtschaftlichen und staatlichen Lebensbereiche hat die Bedeutung von Cybersicherheit in den vergangenen Jahren erheblich gesteigert. Mit der zunehmenden Vernetzung kritischer Systeme, Kommunikationsinfrastrukturen und digitaler Führungs- und Unterstützungsmittel wächst zugleich die Anfälligkeit gegenüber cyberbezogenen Bedrohungen. Sicherheitsvorfälle im digitalen Raum können nicht nur wirtschaftliche und organisatorische Schäden verursachen, sondern auch die Verfügbarkeit, Integrität und Vertraulichkeit sensibler Daten und Systeme beeinträchtigen. Im militärischen Kontext kommt dieser Entwicklung besondere Relevanz zu, da Streitkräfte in hohem Maße von informations- und kommunikationstechnologischen Infrastrukturen abhängig sind und Cyberangriffe hier potenziell unmittelbare Auswirkungen auf Führungsfähigkeit, Einsatzbereitschaft und operationskritische Abläufe entfalten können.

Vor diesem Hintergrund kommt der Ausbildung im Bereich der Cybersicherheit eine zentrale Rolle zu. Sie dient nicht nur dem Aufbau technischer Fachkompetenz, sondern auch der Befähigung militärischen Personals, sicherheitsrelevante Ereignisse zu erkennen, in ihrem Kontext zu bewerten und entsprechend definierter Prozesse angemessen zu reagieren. Cybersicherheitsausbildung ist dabei nicht als einheitliches oder universell standardisiertes Feld zu verstehen. Vielmehr unterscheiden sich Ausbildungsmodelle je nach institutionellem Kontext, nationaler Sicherheitsarchitektur, militärischer Organisationslogik und strategischem Verständnis des Cyberraums als Fähigkeitsbereich. Diese Unterschiede betreffen unter anderem den Grad der Spezialisierung, die organisatorische Einbettung in militärische Bildungsstrukturen, die Verbindung von akademischer und praktischer Ausbildung sowie die Balance zwischen technischen, prozessualen und operativen Ausbildungsinhalten.

Das vorliegende Kapitel betrachtet daher die Cybersicherheitsausbildung im militärischen Sektor im internationalen Vergleich. Ziel ist es, unterschiedliche nationale Modelle, Ausbildungsstrategien und institutionelle Arrangements sichtbar zu machen, um daraus strukturierende Vergleichsdimensionen und potenziell übertragbare Gestaltungsprinzipien abzuleiten. Der Fokus liegt dabei auf ausgewählten Beispielen aus Europa sowie ergänzend auf außereuropäischen Staaten mit erkennbar relevanten militärischen Cyberausbildungsstrukturen. Der Vergleich dient nicht der normativen Bewertung einzelner Länder, sondern der analytischen Einordnung verschiedener Ansätze im Hinblick auf ihre curriculare Struktur, ihren institutionellen Zuschnitt und ihre mögliche Relevanz für die Entwicklung des Projekts Bumblebee.

3.6.1 Ausbildung in Österreich

Die Ausbildung im Bereich der Informations- und Kommunikationstechnologie sowie der Cybersicherheit im österreichischen Bundesheer erfolgt gegenwärtig über mehrere, institutionell miteinander verbundene Ausbildungswege, die sowohl militärische als auch zivile Bildungseinrichtungen einbeziehen. Diese Struktur verweist auf ein Ausbildungsmodell, in dem cyberrelevante Kompetenzen nicht ausschließlich in einem eigenständigen, klar abgegrenzten Ausbildungspfad vermittelt werden, sondern in breitere informations- und kommunikationstechnologische sowie führungsbezogene Ausbildungszusammenhänge eingebettet sind. Einen zentralen Bestandteil der technischen Offiziersausbildung bildet dabei der Fachhochschul-Bachelorstudiengang „Militärische informations- und kommunikationstechnologische Führung“ an der Theresianischen Militärakademie [11]. Dieser Studiengang vermittelt Offiziersanwärterinnen und Offiziersanwärtern grundlegende Kompetenzen im Bereich der Informations- und Kommunikationstechnologien sowie deren Anwendung im militärischen Kontext. Charakteristisch ist dabei, dass die Ausbildung nicht auf die Vermittlung rein

technischer Inhalte beschränkt bleibt, sondern systematisch mit militärischen Führungsfähigkeiten und organisatorischen Aspekten der Einsatzführung verknüpft wird. Damit folgt das Ausbildungsmodell einem integrativen Ansatz, bei dem technisches Fachwissen, militärische Führungsverantwortung und institutionelle Handlungssicherheit in einem gemeinsamen Qualifikationsrahmen zusammengeführt werden [11]. Im Rahmen des Studienprogramms werden unter anderem Inhalte zu Netzwerktechnologien, IT-Infrastruktur, sicheren Informationssystemen sowie zu Grundlagen der Informationssicherheit vermittelt [11]. Diese Themenfelder schaffen Basiskompetenzen, die für den Betrieb, die Überwachung und die organisatorische Einbettung militärischer IT-Systeme von wesentlicher Bedeutung sind. Die Ausbildung zielt dabei nicht allein auf die Beherrschung technischer Werkzeuge oder Systeme ab, sondern insbesondere auf das Verständnis von Systemarchitekturen, Kommunikationsnetzen und sicherheitsrelevanten Prozessen innerhalb militärischer Organisationszusammenhänge. Daraus ergibt sich ein Ausbildungsprofil, das vor allem auf die Verbindung technischer Grundbefähigung mit einem Verständnis militärisch-institutioneller Rahmenbedingungen ausgerichtet ist. Für den Bereich der Cybersicherheit ist dies insofern relevant, als operative Handlungssicherheit im militärischen Kontext nicht nur auf technischer Expertise beruht, sondern ebenso auf der Fähigkeit, technische Beobachtungen in geregelte Führungs-, Melde- und Unterstützungsstrukturen einzubetten [11]. Ein eigenständiger Masterstudiengang im Bereich Cybersicherheit innerhalb des Bundesheeres besteht derzeit nicht. Offiziere, die eine weiterführende akademische Spezialisierung in den Bereichen IT-Security oder Cybersecurity anstreben, müssen entsprechende Masterprogramme an zivilen Hochschulen absolvieren. Der an der Militärakademie erworbene Bachelorabschluss wird jedoch grundsätzlich als Zugangsvoraussetzung für weiterführende akademische Spezialisierungen anerkannt [11]. Dieser Umstand verdeutlicht, dass das österreichische Modell zwar über anschlussfähige Grundlagenstrukturen verfügt, die vertiefte institutionelle Ausdifferenzierung im Bereich der militärischen Cybersicherheitsausbildung jedoch nur begrenzt ausgebaut ist. Die vertikale Entwicklung eines durchgängigen militärischen Ausbildungswegs von der Grundqualifikation bis zur spezialisierten akademischen Vertiefung ist damit bislang nur teilweise innerhalb des Bundesheeres selbst abbildbar [11].

Neben der Offiziersausbildung werden technische und cyberrelevante Inhalte auch an der Führungsunterstützungsschule vermittelt. Dort werden ausgewählte Inhalte der IKT-Ausbildung teilweise in komprimierter Form für andere militärische Zielgruppen aufbereitet. Diese Ausbildungsangebote richten sich insbesondere an Personal, das im operativen Betrieb von IT-Systemen, in technischen Unterstützungsfunktionen oder in informations- und kommunikationstechnologisch geprägten Einsatzbereichen tätig ist [12]. Daraus wird ersichtlich, dass im österreichischen Bundesheer bereits Ansätze bestehen, technische Kompetenzen auch jenseits klassischer Offizierslaufbahnen für breitere Zielgruppen verfügbar zu machen. Zugleich deutet diese Struktur darauf hin, dass Cyberausbildung gegenwärtig eher als Bestandteil allgemeiner technischer Befähigung verstanden wird und weniger als eigenständiger, klar profilierter militärischer Ausbildungsbereich mit spezifisch ausdifferenzierten Rollenprofilen [12].

Insgesamt zeigt das österreichische Modell somit eine institutionelle Grundstruktur, in der cyberrelevante Inhalte durchaus vorhanden sind, jedoch überwiegend in breitere informations- und kommunikationstechnologische Ausbildungsgänge eingebettet bleiben. Ein klar abgegrenzter und durchgängig ausdifferenzierter militärischer Ausbildungspfad im Bereich Cybersicherheit ist bislang nur eingeschränkt erkennbar. Aus wissenschaftlicher Perspektive ist Österreich damit insbesondere als Beispiel für ein System relevant, in dem cyberbezogene Kompetenzen integrativ in bestehende militärisch-technische Ausbildungsstrukturen eingebunden werden, ohne bereits vollständig als eigenständiger Ausbildungsbereich institutionalisiert zu sein [11][12]. Für die vergleichende Betrachtung ist dies insofern aufschlussreich, als sich daran exemplarisch zeigen lässt, dass militärische Cybersicherheitsausbildung auch unter Bedingungen begrenzter institutioneller Spezialisierung stattfinden kann, ihre weitere Professionalisierung jedoch wesentlich

davon abhängt, in welchem Ausmaß cyberbezogene Inhalte künftig organisatorisch, curricular und akademisch eigenständiger verankert werden [11][12].

3.6.2 Ausbildung in Deutschland

In Deutschland erfolgt die militärische Cybersicherheitsausbildung im Kontext des Organisationsbereichs Cyber- und Informationsraum (CIR), der als eigenständiger organisatorischer Rahmen für cyber-, informations- und IT-bezogene Fähigkeiten innerhalb der Bundeswehr fungiert. Bereits diese institutionelle Verankerung verweist auf den hohen Stellenwert, den der Cyberraum im deutschen Verteidigungssystem einnimmt. Innerhalb dieses Organisationsbereichs bestehen spezialisierte Ausbildungsinstitutionen, die unterschiedliche Aufgabenfelder des militärischen Cyber- und Informationsumfelds abdecken. Dazu zählen insbesondere die Schule für Strategische Aufklärung der Bundeswehr sowie die Schule für Informationstechnik der Bundeswehr [13]. Während erstere vor allem Personal für das militärische Nachrichtenwesen und die elektronische Kampfführung ausbildet, konzentriert sich letztere auf die Qualifizierung des IT-Fachpersonals der Streitkräfte [13]. Die Ausbildungslandschaft ist damit durch eine deutliche funktionale Differenzierung gekennzeichnet, die erkennen lässt, dass Cybersicherheitskompetenzen in Deutschland nicht als einheitliches, generalistisches Qualifikationsfeld verstanden werden, sondern als Bündel spezialisierter Fähigkeiten, die je nach Aufgabenprofil unterschiedlich ausgeprägt sein müssen.

Charakteristisch für dieses Modell ist darüber hinaus die Bandbreite der angebotenen Ausbildungsformate. Neben kürzeren Grundkursen, die der Vermittlung elementarer Kompetenzen dienen, werden auch längerfristige spezialisierte Lehrgänge angeboten, deren Ziel darin besteht, die Absolvierenden zur eigenständigen Konfiguration, Administration und Absicherung komplexer Netzwerke und Systeme zu befähigen [13]. Dies verweist auf ein Ausbildungsverständnis, das operative Anwendbarkeit und technische Tiefe miteinander verbindet. Die Ausbildung ist somit nicht allein auf die Vermittlung theoretischer Grundlagen ausgerichtet, sondern auf die Entwicklung konkreter Handlungskompetenzen für den militärischen Betrieb und die Sicherung informations- und kommunikationstechnologischer Systeme. Im Vergleich zu integrativeren oder weniger formal ausdifferenzierten Modellen zeigt sich hier eine institutionelle Logik, in der Cyberkompetenz eng an klar definierte Rollen, Funktionsbereiche und organisationsspezifische Aufgabenprofile gekoppelt ist [13]. Ergänzend zu diesen militärisch-spezifischen Ausbildungsinstitutionen existieren in Deutschland auch akademische Ausbildungsangebote mit unmittelbarer oder mittelbarer Relevanz für den militärischen Cyberbereich. So bietet die Universität der Bundeswehr einen Masterstudiengang im Bereich Cyber-Sicherheit an, der stärker wissenschaftlich ausgerichtet ist und technische mit organisatorischen Aspekten der Informationssicherheit verbindet [14]. Das Studienangebot setzt einschlägige Vorqualifikationen voraus und eröffnet Vertiefungsmöglichkeiten unter anderem in den Bereichen Enterprise Security, Security Intelligence oder Public Security [14]. Damit wird deutlich, dass das deutsche Modell nicht ausschließlich auf praxisorientierte Fachausbildung setzt, sondern auch akademische Spezialisierung als wichtigen Bestandteil der Professionalisierung im Cyberbereich versteht. Die Verknüpfung technischer, organisatorischer und strategischer Perspektiven innerhalb eines universitären Masterprogramms deutet zugleich auf ein breiteres Verständnis von Cybersicherheit hin, das über rein operative Systemverteidigung hinausgeht und auch Governance-, Analyse- und Sicherheitsmanagementaspekte einschließt [14].

Daneben besteht an der Hochschule des Bundes für öffentliche Verwaltung ein Diplomstudiengang „Digitale Administration und Cyber Security“, der auf die Digitalisierung in Bundesbehörden sowie die Abwehr von Cybergefahren ausgerichtet ist [15]. Dieses Angebot richtet sich nicht ausschließlich an Angehörige der Bundeswehr, sondern adressiert breiter den öffentlichen Sektor. Gerade dieser Umstand ist für die vergleichende Betrachtung von besonderem Interesse, da er auf

eine institutionelle Öffnung cyberrelevanter Kompetenzen in Richtung staatlicher Verwaltungs- und Sicherheitskontexte verweist. Cybersicherheitsausbildung erscheint damit nicht ausschließlich als Domäne militärischer Spezialverwendung, sondern als Teil eines umfassenderen staatlichen Kompetenzaufbaus im digitalen Raum [15]. Diese Verschränkung militärischer, behördlicher und akademischer Ausbildungslogiken ist ein zentrales Merkmal des deutschen Modells und unterstreicht die strategische Bedeutung, die cyberbezogenen Fähigkeiten im gesamtstaatlichen Kontext beigemessen wird. Insgesamt zeichnet sich das deutsche Modell durch eine vergleichsweise hohe institutionelle Ausdifferenzierung aus. Besonders auffällig ist die Kombination aus militärisch-spezifischen Schulen, universitärer Spezialisierung und verwaltungsnahen Ausbildungsangeboten, die zusammen ein mehrschichtiges Qualifizierungssystem bilden [13][14][15]. Cybersicherheitsausbildung erscheint hier nicht als singulärer Ausbildungsgang, sondern als komplexes und funktional differenziertes System, das operative, technische, akademische und administrative Anforderungen miteinander verbindet. Aus wissenschaftlicher Perspektive ist Deutschland damit ein besonders aufschlussreiches Beispiel für ein stark institutionalisiertes Ausbildungsmodell, in dem Cyberkompetenzen als eigenständiger Fähigkeitsbereich innerhalb der Streitkräfte und zugleich als Bestandteil gesamtstaatlicher Sicherheits- und Verwaltungskompetenz verankert sind [13][14][15]. Für den internationalen Vergleich ist dies insofern relevant, als sich hier exemplarisch zeigt, wie militärische Cybersicherheitsausbildung durch organisatorische Spezialisierung, akademische Anschlussfähigkeit und institutionelle Breite strukturell gefestigt werden kann.

3.6.3 Ausbildung in Estland

In Estland zeigt sich im Bereich der militärischen Cybersicherheitsausbildung ein Ansatz, der in besonderer Weise durch die enge Verzahnung ziviler IT-Ausbildung mit militärischen Dienststrukturen geprägt ist. Anstatt Cybersicherheit ausschließlich über eigenständige militärische Studiengänge oder umfassend ausdifferenzierte interne Ausbildungsprogramme zu institutionalisieren, wird ein Modell sichtbar, das vorhandene zivile Qualifikationen gezielt mit militärischen Verwendungszusammenhängen verbindet. Ein aktuelles Beispiel hierfür ist die Möglichkeit für IT-Studierende des Kehrna Vocational Education Center, ihr verpflichtendes Berufspraktikum mit dem Wehrdienst im estnischen Cyber Command zu kombinieren [16]. Dadurch kann der Wehrdienst in den regulären Ausbildungsweg integriert werden, ohne dass hierfür zwingend zusätzliche Zeit außerhalb des Studiums aufgewendet werden muss. Voraussetzung für diese Form der Verbindung von ziviler und militärischer Qualifizierung sind bereits vorhandene IT-bezogene Vorkenntnisse sowie die Absolvierung der soldatischen Grundausbildung [16]. Dieser Ansatz ist aus wissenschaftlicher Perspektive insofern bemerkenswert, als er ein flexibles und ressourcenschonendes Modell des Kompetenzaufbaus erkennen lässt. Estland nutzt damit die bestehende Stärke ziviler IT-Ausbildung und überführt sie in militärisch relevante Fähigkeitsprofile, anstatt einen vollständig separaten militärischen Ausbildungspfad für den Cyberbereich aufzubauen. Dadurch entsteht ein Ausbildungssystem, das nicht primär auf institutioneller Trennung, sondern auf funktionaler Anschlussfähigkeit basiert. Der militärische Cyberdienst erscheint in diesem Modell weniger als eigenständige, von zivilen Bildungswegen abgekoppelte Professionalisierungsdomäne, sondern stärker als Anwendungs- und Vertiefungsraum für bereits vorhandene technische Qualifikationen [16]. Diese enge Verbindung zwischen ziviler IT-Kompetenz und militärischer Nutzbarmachung kann insbesondere in kleineren Staaten oder in sicherheitspolitischen Kontexten mit hoher Digitalaffinität als strategisch sinnvoller Ansatz interpretiert werden.

Darüber hinaus bietet die Estonian National Defence Academy Bachelor- und Masterprogramme im militärischen Ausbildungsbereich an. Die verfügbaren Informationen deuten jedoch darauf hin, dass diese Programme nicht primär auf Cybersicherheit spezialisiert sind [17]. Zwar werden innerhalb der Studiengänge vereinzelt Lehrveranstaltungen mit IT- und Security-Bezug angeboten,

ein umfassendes, eigenständiges Cybersecurity-Studium im militärischen Kontext ist daraus jedoch nicht unmittelbar ableitbar [17]. Daraus ergibt sich, dass Cybersicherheitskompetenz im estnischen Modell zwar institutionell präsent ist, jedoch eher als integrierter Bestandteil breiterer militärischer Ausbildungsstrukturen denn als vollständig eigenständiger akademischer Ausbildungspfad erscheint. Die Vermittlung cyberrelevanter Inhalte erfolgt damit offenbar in einer Form, die stärker auf Querschnittsintegration als auf formale Spezialisierung ausgerichtet ist [17]. Für den internationalen Vergleich ist das estnische Modell insbesondere deshalb von Interesse, weil es eine alternative Organisationslogik militärischer Cybersicherheitsausbildung sichtbar macht. Während andere Staaten auf hochgradig institutionalisierte Cyberakademien, spezialisierte militärische Studiengänge oder stark ausdifferenzierte Rollensysteme setzen, scheint Estland stärker auf die systematische Verbindung bestehender ziviler Ausbildungskapazitäten mit militärischen Anwendungsfeldern zu bauen [16][17]. Der Fokus liegt damit weniger auf der Schaffung eines umfangreichen eigenständigen militärischen Cyberhochschulsystems, sondern stärker auf der Integration cyberrelevanter Kompetenzen in bestehende Ausbildungs- und Dienststrukturen. Diese Integrationslogik kann als Ausdruck eines pragmatischen und adaptiven Ausbildungsverständnisses gelesen werden, das institutionelle Anschlussfähigkeit, effiziente Ressourcennutzung und operative Verwendbarkeit miteinander verbindet.

Insgesamt lässt sich Estland somit als Beispiel für ein Modell einordnen, in dem militärische Cybersicherheitsausbildung nicht primär über formale institutionelle Abgrenzung, sondern über die gezielte Kopplung von ziviler Fachqualifikation und militärischer Einsatzfunktion organisiert wird [16][17]. Aus wissenschaftlicher Sicht ist dieser Ansatz besonders aufschlussreich, weil er verdeutlicht, dass die Professionalisierung militärischer Cyberkompetenz nicht zwingend an die Existenz umfangreicher eigenständiger Studiengänge oder exklusiver Ausbildungsinstitutionen gebunden ist. Vielmehr kann sie auch über integrative Strukturen erfolgen, sofern diese in der Lage sind, vorhandene technische Kompetenzen in militärisch anschlussfähige Fähigkeitsprofile zu überführen. Für die vergleichende Analyse liefert Estland damit ein Beispiel für einen flexiblen, integrationsorientierten Ansatz, der insbesondere im Hinblick auf Modularität, Anschlussfähigkeit und Ressourceneffizienz interessante Anknüpfungspunkte für die Entwicklung künftiger Ausbildungsmodelle bietet [16][17].

3.6.4 Ausbildung in Frankreich

Das französische Modell der militärischen Cybersicherheitsausbildung zeichnet sich durch eine vergleichsweise klare institutionelle Struktur, eine starke akademische Verankerung und eine enge Anbindung an die Verteidigungsverwaltung aus. Im Zentrum stehen dabei Ausbildungswege, die über den COMCYBER organisiert beziehungsweise mit dem militärischen Cyberbereich des französischen Verteidigungsministeriums verknüpft sind. Dazu zählt unter anderem das Bachelor-Programm Cybersécurité der EPITA in Partnerschaft mit der École polytechnique, das nach einer dreijährigen Ausbildungsdauer den Einstieg in eine Cyber-Einheit der Streitkräfte als Offizier ermöglicht [18]. Bereits diese Konstellation verweist auf ein Ausbildungsverständnis, das Cybersicherheitskompetenz nicht als bloße Zusatzqualifikation, sondern als eigenständigen professionellen und institutionell eingebetteten Qualifikationspfad begreift. Ergänzend besteht ein Mastère-Programm in Zusammenarbeit mit der École de l'air et de l'espace und Centrale Méditerranée, das sich an Personen mit einem abgeschlossenen Hochschulstudium im Bereich Informatik beziehungsweise an Absolventinnen und Absolventen mit einschlägiger Berufserfahrung richtet [18]. Die Zugangsvoraussetzungen machen deutlich, dass Frankreich im Bereich der militärischen Cybersicherheitsausbildung auch auf eine vertiefte akademische Spezialisierung setzt, die auf bereits vorhandene fachliche Qualifikationen aufbaut. Damit wird Cybersicherheitsausbildung nicht ausschließlich als Grundbefähigung für militärische Funktionen verstanden, sondern zugleich als Gegenstand weiterführender Professionalisierung, der auf unterschiedlichen Qualifikationsniveaus institutionell abgebildet werden kann [18]. Inhaltlich

umfasst die Ausbildung unter anderem Themen zu Netzwerk- und Systemarchitekturen, die für militärische Cyberverteidigung und den sicheren Betrieb digitaler Infrastrukturen von besonderer Bedeutung sind [18]. Diese thematische Ausrichtung verweist auf einen Ausbildungsansatz, der technische Grundlagen nicht isoliert vermittelt, sondern sie in einen sicherheits- und verteidigungsbezogenen Kontext einbettet. Die Relevanz solcher Inhalte ergibt sich insbesondere daraus, dass militärische Cybersicherheitskompetenz auf einem fundierten Verständnis vernetzter Systeme, ihrer potenziellen Verwundbarkeiten und ihrer Rolle innerhalb kritischer digitaler Infrastrukturen beruht. Die Ausbildung zielt damit nicht allein auf technisches Fachwissen, sondern auf die Befähigung, dieses Wissen in institutionell geregelten und sicherheitskritischen Handlungskontexten anzuwenden [18].

Von besonderer Bedeutung ist darüber hinaus das vorgesehene sechswöchige Praktikum im französischen Verteidigungsministerium [18]. Dieses Element verleiht dem französischen Modell eine ausgeprägte Praxisorientierung und stellt sicher, dass die akademisch vermittelten Inhalte nicht losgelöst von den realen Anforderungen des militärischen Cyberbereichs vermittelt werden. Vielmehr entsteht dadurch eine direkte institutionelle Rückbindung an jene Strukturen, in denen die erworbenen Kompetenzen später zur Anwendung kommen sollen. Die praktische Einbindung in ministerielle Kontexte kann insofern als Ausdruck eines Ausbildungsverständnisses gelesen werden, das Theorie, institutionelle Sozialisation und praktische Anwendungsorientierung eng miteinander verknüpft. Für die Qualität und Anschlussfähigkeit militärischer Ausbildung ist dies ein wesentlicher Faktor, da dadurch nicht nur Wissen vermittelt, sondern auch ein Verständnis für organisatorische Prozesse, Zuständigkeiten und sicherheitsrelevante Arbeitskontexte aufgebaut wird [18]. Aus wissenschaftlicher Perspektive ist das französische Modell besonders interessant, weil es mehrere zentrale Merkmale eines formalisierten und professionalisierten militärischen Ausbildungssystems im Cyberbereich miteinander verbindet. Dazu zählen klar strukturierte Ausbildungswege, definierte Zugangsvoraussetzungen, akademische Fundierung, institutionelle Einbettung und praxisnahe Qualifizierung. Im Unterschied zu stärker integrativen Modellen, in denen cyberrelevante Inhalte in breitere IKT- oder Führungsprogramme eingebettet bleiben, erscheint Cybersicherheit hier als eigenständiges und sichtbar profiliertes Ausbildungsfeld mit spezifischen Karriereanschlüssen [18]. Diese institutionelle Klarheit begünstigt nicht nur die curriculare Stringenz, sondern auch die strategische Positionierung des Cyberbereichs als eigenständige militärische Kompetenzdomäne.

Insgesamt lässt sich Frankreich daher als Beispiel für einen akademisch fundierten, institutionell eng angebundenen und vergleichsweise kohärent strukturierten Ansatz militärischer Cybersicherheitsausbildung einordnen [18]. Das Modell zeigt, wie ein Ausbildungsweg ausgestaltet werden kann, der wissenschaftliche Qualifizierung, praktische Erfahrung und organisatorische Einbindung systematisch miteinander verbindet. Für den internationalen Vergleich ist Frankreich insofern besonders aufschlussreich, als hier deutlich wird, dass militärische Cybersicherheitsausbildung dann an Profil und Nachhaltigkeit gewinnt, wenn sie nicht nur inhaltlich spezifiziert, sondern auch organisatorisch, akademisch und institutionell klar verankert ist [18].

3.6.5 Ausbildung in Italien

In Italien ist die militärische Ausbildung im Bereich cyberrelevanter Kompetenzen vor allem in breitere strategische, technische und akademische Ausbildungszusammenhänge eingebettet. Ein zentraler institutioneller Bezugspunkt ist dabei die Scuola di Applicazione, die in Zusammenarbeit mit der Universität Turin verschiedene Masterstudiengänge anbietet, darunter auch Programme mit inhaltlichen Bezügen zur Informatik [19]. In diesem Kontext ist insbesondere das Studienangebot Strategic Military Sciences hervorzuheben, das militärischen Studierenden vorbehalten ist und damit einen spezifischen Rahmen für die Verbindung militärischer Ausbildung mit akademischer Qualifizierung schafft [19]. Bereits diese Struktur deutet darauf hin, dass der

italienische Ansatz weniger auf einen isolierten Cyber-Ausbildungspfad setzt, sondern cyberrelevante Inhalte in umfassendere militärisch-akademische Bildungsformate integriert.

Aus den verfügbaren Informationen lässt sich jedoch kein eigenständiger, klar ausgewiesener militärischer Cybersecurity-Studiengang ableiten [19]. Vielmehr spricht die institutionelle Ausgestaltung dafür, dass die Vermittlung cyberbezogener Kompetenzen in Italien eher in breitere strategische und technische Studienkontexte eingebettet ist, anstatt als separates, formal abgegrenztes Ausbildungsmodell organisiert zu werden. Dies ist aus wissenschaftlicher Perspektive insofern aufschlussreich, als sich hier ein integrativer Zugang erkennen lässt, bei dem Cybersicherheit nicht als singuläre Spezialdomäne, sondern als Bestandteil einer umfassenderen militärischen und technologischen Qualifizierung verstanden wird. Cyberkompetenz erscheint damit eher als Querschnittskompetenz innerhalb moderner Streitkräfte denn als vollständig eigenständiger akademischer Professionalisierungspfad [19]. Diese Einbettung kann sowohl als Stärke als auch als strukturelle Begrenzung interpretiert werden. Einerseits ermöglicht ein integrativer Ansatz, cyberrelevante Themen in größere sicherheits- und verteidigungspolitische Zusammenhänge einzuordnen und sie mit strategischen, organisatorischen und technischen Fragestellungen zu verbinden. Dies kann insbesondere dort von Vorteil sein, wo Cybersicherheit nicht isoliert betrachtet, sondern als Teil eines umfassenderen militärischen Fähigkeitsprofils verstanden wird. Andererseits erschwert das Fehlen eines klar abgegrenzten militärischen Cyberstudiengangs die Sichtbarkeit des Cyberbereichs als eigenständige Ausbildungsdomäne und kann dazu führen, dass Spezialisierungstiefe, curriculare Systematik und institutionelle Profilbildung im Vergleich zu stärker ausdifferenzierten Modellen weniger deutlich ausgeprägt sind [19].

Für den internationalen Vergleich ist Italien daher vor allem als Beispiel für einen integrativen Ausbildungsansatz von Bedeutung. Cyberkompetenzen werden hier offenbar eher in bestehende militärisch-akademische Strukturen eingebettet, statt über ein institutionell eigenständiges und klar sichtbares Cyber-Ausbildungsmodell vermittelt zu werden [19]. Dieses Modell verweist auf eine Organisationslogik, in der die Entwicklung cyberrelevanter Fähigkeiten innerhalb bestehender Bildungs- und Karrierepfade erfolgt und somit stärker an vorhandene militärische Studienformate anschließt, als dass neue spezialisierte Ausbildungsinstitutionen geschaffen werden. Für die vergleichende Analyse ist dies insofern relevant, als sich daran exemplarisch zeigen lässt, dass militärische Cybersicherheitsausbildung auch in Form einer curricularen Integration in übergeordnete strategische und technische Ausbildungszusammenhänge organisiert werden kann. Insgesamt lässt sich das italienische Modell somit als Ausdruck einer eher eingebetteten und weniger stark formal separierten Cybersicherheitsausbildung interpretieren [19]. Aus wissenschaftlicher Sicht ist es insbesondere deshalb interessant, weil es verdeutlicht, dass sich militärische Cyberkompetenz nicht in allen Staaten über eigenständige institutionelle Spezialisierung entwickelt, sondern mitunter als Bestandteil bestehender militärischer Hochschul- und Führungsausbildung aufgebaut wird. Für die Entwicklung von Vergleichsdimensionen im Rahmen des Projekts Bumblebee liefert Italien damit einen wichtigen Referenzfall für die Frage, in welchem Verhältnis eigenständige Cyberinstitutionalisierung und integrative Einbettung zueinander stehen und welche Konsequenzen sich daraus für Profilbildung, Spezialisierungstiefe und curriculare Sichtbarkeit ergeben [19].

3.6.6 Ausbildung in Norwegen

In Norwegen erfolgt die militärische Ausbildung im Bereich Cybersecurity über das Norwegian Defence University College sowie die daran angebundene Norwegian Defence Cyber Academy in Lillehammer [20]. Damit besteht ein institutionalisierter Ausbildungsweg innerhalb des norwegischen Verteidigungssystems, der cyberrelevante Kompetenzen gezielt in die militärische Hochschul- und Offiziersausbildung integriert. Bereits diese organisatorische Verankerung ist für

die vergleichende Betrachtung von besonderer Bedeutung, da sie darauf hindeutet, dass der Cyberbereich innerhalb der norwegischen Streitkräfte nicht lediglich als ergänzendes technisches Themenfeld verstanden wird, sondern als eigenständiger und strategisch relevanter Fähigkeitsbereich institutionell abgebildet ist [20]. Auch wenn aus den vorliegenden Informationen nur begrenzt Details zu curricularer Struktur, Ausbildungsdauer oder einzelnen Lehrinhalten hervorgehen, lässt sich dennoch erkennen, dass Norwegen den Bereich Cyber Defence in klarer organisatorischer Form in das nationale militärische Ausbildungssystem eingebettet hat [20]. Diese Einbettung ist insofern aufschlussreich, als sie auf ein Ausbildungsverständnis verweist, das Cybersicherheit nicht allein als Teil allgemeiner IT-Qualifikation behandelt, sondern als eigenständigen Bestandteil militärischer Professionalisierung. Der Cyberbereich erscheint damit nicht nur als unterstützende technische Funktion, sondern als fest verankerter Bereich militärischer Kompetenzentwicklung, der innerhalb der Verteidigungsorganisation sichtbar institutionell repräsentiert ist [20].

Aus wissenschaftlicher Perspektive ist das norwegische Modell insbesondere deshalb interessant, weil es zeigt, dass bereits die klare organisatorische Verankerung von Cyberausbildung einen wesentlichen Indikator für den Stellenwert dieses Fähigkeitsfeldes darstellen kann. Selbst wenn die öffentlich verfügbaren Informationen zu konkreten Curricula begrenzt sind, spricht die institutionelle Einbindung in eine militärische Hochschulstruktur dafür, dass Cybersicherheitskompetenz in Norwegen als systematisch entwickelbare Qualifikation verstanden wird, die in enger Verbindung zu militärischer Führung, akademischer Ausbildung und nationaler Verteidigungsfähigkeit steht [20]. Damit unterscheidet sich Norwegen von stärker integrativen Modellen, in denen cyberrelevante Inhalte zwar vermittelt werden, jedoch nicht in gleicher Weise sichtbar und organisatorisch eigenständig verankert sind. Für den internationalen Vergleich ist Norwegen somit als Beispiel für einen hochschulisch verankerten militärischen Cyber-Ausbildungsansatz relevant, bei dem Cyber Defence als eigenständiger Bestandteil der nationalen Verteidigungsorganisation geführt wird [20]. Das Modell verdeutlicht, dass die Qualität und Nachhaltigkeit militärischer Cybersicherheitsausbildung nicht ausschließlich von der Breite öffentlich sichtbarer Curricula oder der Zahl einzelner Studiengänge abhängen, sondern wesentlich auch von der institutionellen Klarheit, mit der der Cyberbereich in Ausbildung, Organisation und Fähigkeitsentwicklung eingebunden ist. Für das Projekt Bumblebee ist dies insofern aufschlussreich, als sich daraus die Bedeutung einer klaren organisatorischen Zuordnung und einer nachvollziehbaren institutionellen Verankerung für die langfristige Tragfähigkeit eines Ausbildungsformats ableiten lässt [20].

3.6.7 Ausbildung in der Schweiz

Die Schweiz verfügt mit dem Cyber Bataillon 42 und dem Kommando Cyber über eine institutionell klar erkennbare Struktur zur Entwicklung militärischer Cyberfähigkeiten. Die militärischen Cyberspezialistinnen und Cyberspezialisten werden in diese Formationen eingeteilt und unterstützen das Kommando Cyber „in allen Lagen“. Damit ist Cybersicherheit innerhalb der Schweizer Armee nicht lediglich als ergänzende IT-Kompetenz organisiert, sondern als eigenständiger militärischer Fähigkeitsbereich mit spezifischer organisatorischer Verankerung [21]. Diese institutionelle Sichtbarkeit ist für den internationalen Vergleich besonders relevant, da sie darauf verweist, dass Cyberkompetenz in der Schweizer Armee nicht nur technisch, sondern auch strukturell und laufbahnbezogen verankert wird. Der Zugang zu diesem Fähigkeitsbereich erfolgt insbesondere über den Cyber-Lehrgang, der nach Angaben der Schweizer Armee 800 Unterrichts- und Praktikumsstunden umfasst und als Teil der entsprechenden militärischen Ausbildung in Jassbach durchgeführt wird [21]. Ergänzende aktuelle Informationen der Schweizer Armee zeigen, dass dieser Lehrgang nach einer Selektion während der Rekrutenschule in einen 40-wöchigen Ausbildungsweg überführt werden kann, der neben umfangreicher technischer Ausbildung auch die Führungsausbildung zum Wachtmeister beinhaltet [22]. Bereits diese Ausbildungsdauer deutet

im internationalen Vergleich auf einen hohen Professionalisierungsgrad sowie auf den Anspruch hin, Cyberkompetenz nicht nur punktuell, sondern systematisch und nachhaltig aufzubauen. Die Ausbildung ist damit deutlich umfangreicher als kurzfristige Einführungskurse und weist Merkmale eines strukturierten, funktionsbezogenen Qualifizierungspfads auf.

Inhaltlich ist das Schweizer Modell bemerkenswert breit angelegt. Zu den ausgewiesenen Aufgaben militärischer Cyberspezialistinnen und Cyberspezialisten zählen unter anderem die Entwicklung von Softwarewerkzeugen, die Analyse von Cyberereignissen und -attacken, die Schwachstellenanalyse, das Incident Management, technische und forensische Untersuchungen, die Lageanalyse und -darstellung sowie die technische, beratende und ausbildende Unterstützung von Truppen im Feld [21][22]. Hinzu kommt, dass die Milizangehörigen ihren Dienst in den drei Fachbereichen Cyberabwehr, militärisches Cyberlagebild und Kryptologie leisten [21]. Diese Kombination aus technischer Analysefähigkeit, Lagebildkompetenz, forensischen Anteilen und feldnaher Unterstützungsleistung verweist auf ein Ausbildungsverständnis, das Cyber nicht nur als Schutz digitaler Systeme, sondern als operativ relevante Unterstützungsfunktion innerhalb militärischer Gesamtstrukturen begreift. Gerade diese Verbindung von Cyberabwehr, Lagebildarbeit und Truppenunterstützung macht das Schweizer Modell aus wissenschaftlicher Sicht besonders interessant, da hier technische Spezialisierung und operative Einbettung in auffälliger Weise zusammengeführt werden. Darüber hinaus weist das Schweizer Modell eine ausgeprägte Anschlussfähigkeit an zivile Bildungs- und Qualifikationswege auf. Nach erfolgreichem Abschluss des Cyber-Lehrgangs besteht eine vereinfachte Zulassung zur Berufsprüfung „Cyber Security Specialist“ mit eidgenössischem Fachausweis; neuere Angaben der Schweizer Armee verweisen zudem darauf, dass diese Berufsprüfung seit 2026 bereits während des Lehrgangs absolviert werden kann [21][22]. Ergänzend eröffnet der absolvierte Lehrgang vereinfachte Zugänge zu ausgewählten Hochschulen sowie Perspektiven für Weiterbildungen im In- und Ausland [21]. Diese Durchlässigkeit zwischen militärischer Ausbildung, ziviler Anerkennung und weiterführender Professionalisierung ist im internationalen Vergleich ein wesentliches Strukturmerkmal. Insgesamt lässt sich die Schweiz daher als Beispiel für ein stark anwendungsorientiertes, institutionell klar verankertes und zugleich zivil anschlussfähiges Modell militärischer Cybersicherheitsausbildung einordnen. Für die vergleichende Analyse ist dies insofern bedeutsam, als das Schweizer Modell zeigt, wie militärische Cyberausbildung technische Tiefe, operative Unterstützungsleistung, Führungsausbildung und zivil verwertbare Qualifizierung in einem kohärenten Ausbildungsrahmen verbinden kann [21][22].

3.6.8 Ausbildung in den USA

Die Vereinigten Staaten verfügen im internationalen Vergleich über ein besonders breit ausgebautes, institutionell stark ausdifferenziertes und funktionsbezogen strukturiertes System militärischer Cybersicherheitsausbildung. Dies zeigt sich insbesondere am Beispiel der U.S. Army, in der Cyberfähigkeiten nicht als bloßes Zusatzfeld klassischer IT-Ausbildung verstanden werden, sondern als eigenständiger militärischer Fähigkeitsbereich mit klarer organisatorischer Verankerung. So beschreibt die U.S. Army ihr Cyber Corps ausdrücklich als Bereich, in dem Soldatinnen und Soldaten sowie Offiziere spezialisierte Ausbildungen für das Betreiben und Verteidigen militärischer Netzwerke, für Cyber Warfare und für elektromagnetische Operationen erhalten [22]. Ergänzend verweist die U.S. Army Cyber Command darauf, dass cyberspace operations, electromagnetic warfare und information operations integraler Bestandteil der militärischen Operationsführung sind und dass die Army hierzu bereits heute weltweit einsetzbare Kräfte vorhält [22]. Diese institutionelle Einbettung macht deutlich, dass Cybersicherheit in den USA nicht nur als Schutzfunktion, sondern als eigenständige operative Domäne mit defensiven und offensiven Komponenten verstanden wird.

Besonders charakteristisch für das US-amerikanische Modell ist die starke rollenbezogene Differenzierung. Die Army weist eigene Karriereprofile und Ausbildungspfade unter anderem für Cyber Operations Specialists, Cyber Warfare Officers sowie für Funktionen im Bereich Electromagnetic Warfare aus [22]. Diese Rollen unterscheiden sich nicht nur hinsichtlich Zugangsvoraussetzungen und Laufbahnlogik, sondern auch im Hinblick auf ihre funktionale Einbindung in militärische Operationen. Die Ausbildung umfasst nach offiziellen Angaben grundlegende technische, elektromagnetische und cyberwarfare-bezogene Fähigkeiten, den Erwerb von Programmier- und Softwareentwicklungskenntnissen, fortgeschrittene Inhalte wie Malware-Analyse, Computer Forensics und Hacking sowie Führungs- und Electronic-Warfare-Anteile [22]. Daraus wird ersichtlich, dass das US-Modell im Unterschied zu stärker defensiv oder administrativ geprägten Ausbildungsansätzen ein deutlich breiteres Kompetenzverständnis verfolgt, das operative, technische und zum Teil offensive Elemente systematisch miteinander verbindet. Eine zentrale Rolle in diesem System spielt die U.S. Army Cyber School, die innerhalb des Cyber Center of Excellence für die fachliche Ausbildung und Professionalisierung von Offizieren, Warrant Officers und Enlisted Personnel verantwortlich ist. Nach offiziellen Angaben ist die Cyber School für die Aus- und Weiterbildung in den Bereichen Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Electromagnetic Warfare (EW) sowie für cyberspace planning, integration and synchronization zuständig [23]. Das übergeordnete Cyber Center of Excellence fungiert zugleich als proponent institution für Cyberspace Operations, Signal/Communications Networks and Information Services sowie Electronic Warfare und verbindet damit Doktrin, Ausbildung, Organisationsentwicklung und Personalentwicklung in einem gemeinsamen institutionellen Rahmen [23]. Aus wissenschaftlicher Perspektive ist dies besonders bedeutsam, da hier sichtbar wird, wie militärische Cybersicherheitsausbildung nicht isoliert als Kursangebot, sondern als Teil eines umfassenden Fähigkeits- und Professionalisierungssystems organisiert wird. Ergänzt wird diese Struktur durch den Cyber Technical College, der auf die technische Initial- und Funktionsausbildung spezialisiert ist. Nach Angaben des Cyber Center of Excellence umfasst dessen Kursangebot unter anderem die Cyber Operations Specialist Advanced Individual Training, den Cyber Basic Officer Leadership Course, den Cyber Operations Officer Course sowie Lehrgänge im Bereich Electromagnetic Warfare [24]. Parallel dazu existiert mit dem Cyber Leader College eine Einrichtung, die stärker auf Professional Military Education und weiterführende Laufbahnentwicklung für Cyber- und EW-Personal ausgerichtet ist. Diese institutionelle Zerteilung zwischen technischer Grund- und Funktionsausbildung einerseits sowie laufbahnbezogener Führungs- und Weiterqualifizierung andererseits verweist auf einen hohen Grad an Professionalisierung und Spezialisierung innerhalb des US-amerikanischen Systems [24]. Im internationalen Vergleich ist dies ein markantes Merkmal, da hier nicht nur Inhalte, sondern auch Ausbildungsebenen und Karrierephasen systematisch voneinander differenziert werden.

Neben den inner-militärischen Ausbildungsstrukturen bestehen in den USA darüber hinaus ausgeprägte Anschlussbeziehungen an den akademischen Sektor. Ein wichtiges Beispiel ist die Partnerschaft zwischen dem U.S. Army Cyber Center of Excellence und der University of Maryland Global Campus (UMGC). Nach Angaben der UMGC können Teilnehmende der Cyber School im Rahmen dieses Degree-Program-Partnerschaftsmodells militärische Ausbildung und Berufserfahrung auf ein Bachelorstudium im Bereich computer networks and cybersecurity anrechnen lassen; für Besuchende der Cyber School sind dabei bis zu 51 Transfer Credits ausgewiesen [25]. Diese Durchlässigkeit zwischen militärischer Fachausbildung und akademischer Qualifizierung ist aus vergleichender Perspektive besonders relevant, da sie zeigt, dass das US-Modell nicht nur auf kurzfristige Einsatzbefähigung zielt, sondern auch längerfristige Professionalisierungs- und Bildungswege strukturell unterstützt. Damit entsteht ein Ausbildungssystem, das operative Verwendbarkeit und akademische Anschlussfähigkeit in institutionell geregelter Weise miteinander verknüpft. Darüber hinaus existiert in den Vereinigten Staaten ein breiteres, verteidigungsnahes Weiterbildungssystem, das das militärische Ausbildungssystem ergänzt, ohne selbst Teil der Streitkräfte zu sein. Hierzu zählen etwa die

Angebote des SANS Institute, das für den öffentlichen Sektor und ausdrücklich auch für Defense and Intelligence sowie den Department of Defense mission-orientierte Cybertrainings, Cyber Ranges und DoD-8140-bezogene Weiterbildungspfade anbietet [26]. Solche Angebote sind für die vergleichende Analyse insofern relevant, als sie zeigen, dass militärische und verteidigungsnahe Cyberqualifizierung in den USA nicht ausschließlich innerhalb der Streitkräfte selbst erfolgt, sondern durch spezialisierte externe Anbieter mit starkem Praxis- und Einsatzbezug ergänzt wird. Hinzu kommen föderale Such- und Weiterbildungsinfrastrukturen wie der NICCS Education and Training Catalog der CISA, der als landesweite Plattform Cyberkurse verschiedener Anbieter bündelt und entlang des NICE Framework strukturiert zugänglich macht [27]. Auch wenn diese Angebote nicht mit inner-militärischer Laufbahnausbildung gleichzusetzen sind, verdeutlichen sie, wie stark der Aufbau cyberbezogener Qualifikationen in den USA in ein breites institutionelles Ökosystem aus Militär, Hochschulen, Bundesbehörden und spezialisierten Trainingsanbietern eingebettet ist. Insgesamt lässt sich das US-amerikanische Modell damit als hochgradig ausdifferenziertes, mehrstufiges und institutionell breit abgestütztes System militärischer Cybersicherheitsausbildung charakterisieren. Kennzeichnend sind insbesondere die klare organisatorische Verankerung des Cyberbereichs, die starke Rollendifferenzierung, die systematische Trennung von Grund-, Funktions- und Führungsqualifizierung, die Einbindung offensiver und elektromagnetischer Fähigkeitsanteile sowie die ausgeprägte Anschlussfähigkeit an akademische und verteidigungsnahe Weiterbildungssysteme [22][23][24][25][26][27]. Für den internationalen Vergleich ist das US-Modell deshalb von besonderem Interesse, weil es die weitreichendste Institutionalisierung militärischer Cyberausbildung unter den betrachteten Staaten erkennen lässt. Für das Projekt Bumblebee eignet es sich allerdings weniger als direkt übertragbare Vorlage denn als Referenzfall dafür, wie umfassend ein militärisches Ausbildungssystem ausgebaut werden kann, wenn Cyber als eigenständiger Operationsraum und als strategischer Fähigkeitsbereich verstanden wird.

3.6.9 Ausbildung in Kanada

In Kanada ist die militärische Cybersicherheitsausbildung als mehrstufiges Qualifizierungssystem ausgestaltet, das militärische Grundausbildung, technische Fachausbildung, institutionalisierte Cyber-Force-Generation und akademische Weiterqualifizierung miteinander verbindet. Einen zentralen Bezugspunkt bildet dabei die Laufbahn des Cyber Operator innerhalb der Canadian Armed Forces (CAF). Der Einstieg erfolgt über die Basic Military Qualification (BMQ), also die militärische Grundausbildung, an die sich eine fachspezifische Ausbildung im Bereich Netzwerksicherheit anschließt. Nach aktuellen offiziellen Angaben absolvieren Cyber Operators anschließend ein CAF-approved college program on computer network security sowie einen etwa 16-wöchigen Lehrgang an der Canadian Forces School of Communications and Electronics (CFSCE) in Kingston. Dort werden Inhalte wie Cyber Operations, Datenerfassung und statistische Analyse, Kommunikations- und Datensicherheit sowie der Betrieb unterstützender technischer Systeme vermittelt [28]. Ergänzend weisen aktuelle Informationen darauf hin, dass die Cyber Training Unit (CTU) unter dem Canadian Armed Forces Cyber Command (CAFCYBERCOM) die Force Generation der Cyber Operators führt und seit 2025 eine neue foundational training pipeline in Partnerschaft mit dem Algonquin College aufgebaut wurde, um den Übergang von Grundlagenwissen zu operationeller Verwendungsfähigkeit stärker zu strukturieren [28]. Diese Entwicklung verweist auf einen Professionalisierungsschub innerhalb des kanadischen Modells, in dem Cyberausbildung zunehmend als eigenständiger militärischer Fähigkeitsbereich organisatorisch gebündelt wird. Inhaltlich zeigt sich, dass das kanadische Modell die Ausbildung nicht auf allgemeine IT-Kompetenz beschränkt, sondern auf ein rollenbezogenes Profil zuschneidet, das defensive Cyberoperationen, Netzwerküberwachung, Analysefähigkeit und die Reaktion auf sicherheitsrelevante Ereignisse umfasst. Nach offizieller Beschreibung sammeln, verarbeiten und analysieren Cyber Operators Netzwerkdaten, identifizieren Schwachstellen, verwalten Netzwerkinfrastrukturen und führen defensive sowie – sofern erforderlich und möglich –

aktive Cyberoperationen durch [28]. Darüber hinaus können spezialisierte Fähigkeitsprofile etwa in den Bereichen Digital Forensics, Threat Intelligence Analysis, Malware Identification and Analysis, Network Vulnerability Evaluations und Cyber Event Mitigation aufgebaut werden [28]. Aus wissenschaftlicher Perspektive ist dies besonders aufschlussreich, weil sich hier ein Ausbildungsverständnis erkennen lässt, das zwischen Grundqualifikation und nachgelagerter Spezialisierung differenziert. Kanada folgt damit weder einem ausschließlich akademischen noch einem rein kasuistisch-praktischen Modell, sondern verbindet militärische Basisausbildung mit einer schrittweise vertieften cyberfachlichen Professionalisierung. Zugleich unterstreicht die 2024/2025 erfolgte institutionelle Bündelung im CAF CYBERCOM, dass Cyberfähigkeiten in den kanadischen Streitkräften inzwischen als strategisch relevanter, eigenständig organisierter Operations- und Unterstützungsbereich behandelt werden [28].

Neben dieser militärischen Berufsausbildung verfügt Kanada auch über ausgeprägte akademische Anschluss- und Vertiefungspfade. Das Royal Military College of Canada (RMC) führt ein institutionell breit angelegtes Cyber Programme, das nach eigenen Angaben Komponenten auf Undergraduate-, Graduate- und Professional-Military-Education-Ebene umfasst [29]. Auf Graduate-Level sind unter anderem Master of Applied Science, Master of Engineering sowie Doctoral-Programme mit Spezialisierung in Cyber Security vorgesehen; darüber hinaus können auch in Programmen wie War Studies, Defence Studies, MBA und MPA Forschungsarbeiten beziehungsweise Kurse mit Cyber-Security-Bezug absolviert werden [29]. Ergänzt wird dies durch ein Graduate Diploma in Cyber Security, das als nichtgradverleihendes, aber anschlussfähiges Programm ausgestaltet ist [29]. Auf Undergraduate-Ebene enthält etwa der Studiengang Computer Engineering mehrere Kern- und Wahlfächer im Bereich Cyber Security [29]. Diese akademische Breite ist für den internationalen Vergleich besonders relevant, da sie zeigt, dass Kanada nicht nur operative Cyberkräfte ausbildet, sondern zugleich wissenschaftlich orientierte Karriere- und Forschungswege im Cyberbereich innerhalb militärischer Bildungsstrukturen institutionell absichert. Hinzu kommen Kurz- und Weiterbildungsformate im Rahmen der militärischen Weiterbildung. Das RMC Cyber Programme bietet eine Reihe von Professional Military Education (PME) short courses an, die sich an Angehörige der Canadian Armed Forces, des Department of National Defence sowie weiterer Regierungsstellen richten [30]. Diese Kurse sind Teil eines Professional Certificate in Cyber Security Foundations und verweisen damit auf ein System, das nicht nur Erstausbildung, sondern auch kontinuierliche Qualifikationsentwicklung unterstützt [30]. Insgesamt lässt sich das kanadische Modell daher als mehrstufiges, institutionell vernetztes und in besonderer Weise durchlässiges Ausbildungssystem charakterisieren. Es kombiniert militärische Grundausbildung, spezialisierte technische Fachausbildung, organisatorisch gebündelte Force Generation im Cyberbereich, akademische Vertiefung und berufsbegleitende Weiterbildung [28][29][30]. Für die vergleichende Analyse ist Kanada damit insbesondere als Beispiel für ein Modell aufschlussreich, das operative Verwendbarkeit und wissenschaftliche Anschlussfähigkeit in strukturierter Weise miteinander verbindet. Im Unterschied zu rein integrativen Modellen ist hier eine deutlichere Institutionalisierung des Cyberbereichs erkennbar; zugleich bleibt das System offen für unterschiedliche Professionalisierungsniveaus und Karrierepfade, was es für die Ableitung modularer Ausbildungslogiken im Kontext von Bumblebee besonders interessant macht.

3.6.10 Ausbildung im Vereinigten Königreich

Im Vereinigten Königreich ist die militärische Cybersicherheitsausbildung nicht primär in einem einheitlichen, generalistischen Cyber-Ausbildungspfad organisiert, sondern in mehrere spezialisierte Rollenprofile eingebettet, die sich auf unterschiedliche institutionelle Träger und Fähigkeitsbereiche verteilen. Besonders relevant sind dabei einerseits das Intelligence Corps mit den Laufbahnen Operator Military Intelligence [32] und Operator Technical Intelligence [33] sowie andererseits das Royal Signals, in dem cyber- und informationsbezogene Kompetenzen unter anderem im Berufsbild des Cyber Engineer beziehungsweise der auf der aktuellen Army-Jobs-

Seite als Communications Engineer geführten Rolle [31] sowie im Bereich Electronic Warfare & Signals Intelligence [34] verankert sind. Offizielle Angaben der British Army zeigen zudem, dass das Intelligence Corps seine Laufbahnen ausdrücklich in drei Karrierepfade gliedert, darunter Operator Military Intelligence als Primärlaufbahn und Operator Technical Intelligence als Speziallaufbahn mit Fokus auf Signals Intelligence, Cyber oder Sprachen [32][33]. Aus wissenschaftlicher Perspektive verweist diese Struktur auf ein Ausbildungsmodell, in dem Cyberkompetenz nicht als isolierte Fachdomäne erscheint, sondern eng mit militärischer Nachrichtenanalyse, Kommunikationssystemen, Signals Intelligence und elektronischer Kampfführung verflochten ist. Das britische Modell ist damit weniger durch institutionelle Zentralisierung als durch rollenbezogene Differenzierung charakterisiert.

Eine wichtige Rolle innerhalb dieses Systems nimmt das im Royal Signals verankerte technische Berufsfeld ein, das in der von dir zitierten Referenz [31] cyberbezogen gefasst ist und aktuell auf der offiziellen Army-Jobs-Seite als Communications Engineer beschrieben wird. Dieses Berufsbild ist in drei Spezialisierungen gegliedert: Network Engineer, Information Services Engineer und Communications Infrastructure Engineer [31]. Die Ausbildung beginnt mit der militärischen Grundausbildung und wird anschließend durch eine technische Ausbildungsphase ergänzt, in der grundlegende Signalling- und Kommunikationsfähigkeiten, der Umgang mit militärischen Funk- und Netzwerksystemen sowie Sicherheitsaspekte einschließlich Cyber vermittelt werden [31]. Besonders hervorzuheben ist, dass diese Rolle nicht allein auf klassische Fernmeldetechnik abzielt, sondern die Schutz- und Betriebsfähigkeit militärischer Netzwerke und Informationssysteme systematisch mitdenkt. Daraus ergibt sich ein Ausbildungsverständnis, in dem cyberrelevante Kompetenzen eng mit Kommunikationsinfrastruktur, Netzwerkbetrieb und sicherer Informationsverarbeitung verbunden sind. Das britische Modell weist damit im Bereich Royal Signals eine deutliche Nähe zwischen Kommunikations- und Cyberausbildung auf, ohne diese notwendigerweise vollständig in einen eigenständigen Cyberstudiengang zu überführen. Innerhalb des Intelligence Corps zeigen die Rollen Operator Military Intelligence [32] und Operator Technical Intelligence [33], dass Cyberkompetenzen im Vereinigten Königreich zugleich stark nachrichtendienstlich und analysebezogen gerahmt werden. Der Operator Military Intelligence sammelt und analysiert Informationen zur Unterstützung militärischer Entscheidungsprozesse und kann dabei nach offiziellen Angaben unter anderem auch Vorgesetzte über einen Cyberangriff briefen [32]. Die Ausbildung umfasst nach der militärischen Grundausbildung eine 15-wöchige Phase-2-Ausbildung am Joint Intelligence Training Group bei Bedford, in der analytische und intelligence-bezogene Fähigkeiten aufgebaut werden [32]. Der Operator Technical Intelligence ist demgegenüber explizit als Speziallaufbahn mit Fokus auf Signals Intelligence, Cyber oder Languages ausgewiesen [33]. Laut offizieller Beschreibung dauert die Ausbildung in dieser Rolle rund zwei bis drei Jahre und umfasst nach der militärischen Grundausbildung zunächst einen 15-wöchigen Kurs in den Grundlagen technischer Intelligenzanalyse, gefolgt von weiteren Ausbildungsanteilen in Analyse, Cyber Skills und/oder operativen Sprachen, die je nach Spezialisierung zwischen drei und 18 Monaten dauern können; für Linguisten kommt zusätzlich ein intensiver Sprachlehrgang hinzu [33]. Diese Struktur macht deutlich, dass der britische Ansatz Cyber nicht nur als technische Schutzaufgabe betrachtet, sondern auch als Teil eines erweiterten intelligence-orientierten Fähigkeitsfeldes, in dem Analyse, SIGINT, operative Sensitivität und gegebenenfalls sprach- und kulturbezogene Komponenten miteinander verbunden werden.

Besonders ausgeprägt wird die Verknüpfung von Cyber, Kommunikationstechnik und militärischer Operationsunterstützung schließlich im Bereich Electronic Warfare & Signals Intelligence [34]. Die offizielle Rollenbeschreibung hebt hervor, dass EWSI-Operatoren im Rahmen von information warfare gegnerische Kommunikation ausnutzen und stören, gegnerische persönliche Kommunikationsmittel, Satellitensysteme, komplexe Radarsysteme und Steuerverbindungen unbemannter Systeme adressieren sowie mit Special Forces, Strategic Intelligence Partners und Verbündeten zusammenarbeiten [34]. Bereits diese Funktionsbeschreibung macht deutlich, dass

das britische Modell über eine rein defensive Cybersicherheitsausbildung hinausgeht und den Cyber- und Informationsraum als eng mit elektronischer Kampfführung, Signals Intelligence und operativer Wirkungserzeugung verbunden begreift. Insgesamt lässt sich das Vereinigte Königreich daher als Beispiel für ein stark rollenorientiertes, funktional differenziertes und institutionell verteiltes Ausbildungsmodell charakterisieren, in dem Cyberkompetenzen über mehrere Laufbahnen hinweg aufgebaut werden. Für die vergleichende Analyse ist dies besonders aufschlussreich, weil hier sichtbar wird, dass militärische Cybersicherheitsausbildung auch ohne ein einziges, zentralisiertes Cybercurriculum hochgradig spezialisiert organisiert werden kann — vorausgesetzt, Rollenprofile, Ausbildungslogiken und institutionelle Zuständigkeiten sind klar definiert. Für das Projekt Bumblebee ist das britische Modell daher vor allem im Hinblick auf die modulare Zuordnung von Kompetenzen zu konkreten Einsatzrollen sowie auf die Verbindung von technischer, nachrichtendienstlicher und prozessualer Ausbildung relevant.

3.6.11 Vergleichende Einordnung und Implikationen für Bumblebee

Der internationale Vergleich zeigt, dass militärische Cybersicherheitsausbildung institutionell, curricular und funktional sehr unterschiedlich ausgestaltet sein kann, sich jedoch entlang mehrerer wiederkehrender Strukturmerkmale systematisch vergleichen lässt. Zu diesen Vergleichsdimensionen zählen insbesondere der Grad der organisatorischen Eigenständigkeit des Cyberbereichs, die Tiefe der fachlichen Spezialisierung, die curriculare Verzahnung mit militärischer Grund- und Führungsausbildung, das Verhältnis von akademischer und praxisorientierter Qualifizierung sowie die Balance zwischen technischen, operativen und prozessual-organisatorischen Ausbildungsinhalten. Die betrachteten Beispiele machen deutlich, dass militärische Cybersicherheitsausbildung kein einheitliches Modell kennt, sondern in Abhängigkeit von nationalen Verteidigungsstrukturen, sicherheitspolitischen Prioritäten und institutionellen Traditionen in sehr unterschiedlichen Formen realisiert wird [11]-[34].

Ein erster zentraler Befund betrifft den Grad der Institutionalisierung. Staaten wie die USA, Deutschland, Frankreich, Kanada oder die Schweiz verfügen über vergleichsweise klar erkennbare organisatorische Strukturen, in denen Cyberkompetenzen als eigenständiger Fähigkeitsbereich sichtbar verankert sind [13]-[15][18][21]-[30]. In diesen Modellen ist Cybersicherheitsausbildung nicht bloß Bestandteil allgemeiner IT-Qualifizierung, sondern Teil eines explizit benannten und institutionell abgesicherten Ausbildungs- und Laufbahnsystems. Demgegenüber zeigen Österreich, Estland, Italien und teilweise auch Norwegen stärker integrative oder hybrid strukturierte Modelle, in denen cyberrelevante Inhalte zwar vorhanden sind, jedoch teilweise in breitere informations- und kommunikationstechnologische, militärisch-akademische oder zivile Ausbildungszusammenhänge eingebettet bleiben [11][12][16][17][19][20]. Dieser Unterschied ist für die vergleichende Analyse bedeutsam, weil er darauf verweist, dass der Reifegrad militärischer Cybersicherheitsausbildung nicht allein an einzelnen Kursen oder Studienangeboten festgemacht werden kann, sondern wesentlich von der institutionellen Sichtbarkeit und organisatorischen Klarheit des Cyberbereichs abhängt.

Ein zweiter wesentlicher Vergleichsaspekt betrifft die Tiefe der Spezialisierung und Rollendifferenzierung. Besonders ausgeprägt ist diese in den USA und im Vereinigten Königreich, wo unterschiedliche Cyber-, Intelligence-, Electromagnetic-Warfare- und technische Laufbahnen mit jeweils eigenen Ausbildungslogiken bestehen [22]-[27][31]-[34]. Auch Deutschland weist mit seinen spezialisierten Schulen und akademischen Vertiefungsangeboten eine deutliche funktionale Differenzierung auf [13]-[15]. Demgegenüber stehen Modelle wie Österreich oder Italien, in denen cyberrelevante Kompetenzen eher als Teil breiterer militärisch-technischer oder strategischer Ausbildungsprofile vermittelt werden [11][12][19]. Die Schweiz und Kanada nehmen in diesem Vergleich eine Zwischenposition ein: Beide Systeme verfügen über klar erkennbare cyberbezogene Ausbildungspfade, verbinden diese jedoch stark mit operativer Anwendbarkeit,

technischer Unterstützungsleistung und anschlussfähigen Weiterbildungsoptionen [21][22][28]-[30]. Insgesamt zeigt sich, dass militärische Cybersicherheitsausbildung entweder über stark spezialisierte Rollenprofile oder über integrativ angelegte Grundqualifikationen organisiert werden kann. Welche Form gewählt wird, hängt dabei erkennbar vom jeweiligen nationalen Verständnis des Cyberraums als eigenständiger Operationsdomäne, Unterstützungsfunktion oder Querschnittsbereich ab.

Ein dritter Vergleichspunkt betrifft das Verhältnis von akademischer Qualifizierung und praxisnaher Funktionsausbildung. Frankreich, Deutschland, Kanada und teilweise die USA weisen eine starke akademische Verankerung der Cyberausbildung auf, indem sie Bachelor-, Master- oder weiterführende Studienangebote mit militärischem oder sicherheitsbezogenem Bezug bereitstellen [14][18][25][29]. Diese Modelle ermöglichen eine vertiefte fachliche Spezialisierung und schaffen zugleich institutionelle Anschlussfähigkeit an Hochschul- und Forschungskontexte. Andere Systeme, etwa die Schweiz oder das Vereinigte Königreich, betonen demgegenüber stärker die praxis- und rollenorientierte Ausbildung, auch wenn dort ebenfalls zivil anerkannte Weiterbildungs- oder Qualifizierungswege bestehen [21][22][31]-[34]. Estland wiederum zeigt exemplarisch, dass militärische Cyberkompetenz auch über die enge Verzahnung ziviler IT-Ausbildung mit militärischem Dienst aufgebaut werden kann [16][17]. Aus vergleichender Perspektive wird damit deutlich, dass akademische Formalisierung und operative Anwendungsorientierung keine Gegensätze sein müssen, sondern in unterschiedlich starker Gewichtung nebeneinander bestehen können. Entscheidend ist weniger die exakte institutionelle Form als vielmehr die Frage, ob zwischen Grundlagenvermittlung, praktischer Anwendung und weiterführender Professionalisierung ein nachvollziehbarer Entwicklungszusammenhang besteht.

Ein weiterer zentraler Befund ergibt sich aus der inhaltlichen Schwerpunktsetzung der betrachteten Modelle. Während einige Staaten, insbesondere die USA und das Vereinigte Königreich, Cyberausbildung eng mit offensiven Fähigkeiten, elektronischer Kampfführung, Signals Intelligence und operationsbezogenen Wirkungsformen verknüpfen [22]-[27][31]-[34], legen andere Systeme den Schwerpunkt stärker auf defensive Cyberfähigkeiten, Netzwerkschutz, Incident Response, Lagebildarbeit und feldnahe Unterstützung [18][21][22][28]-[30]. Österreich und Deutschland zeigen darüber hinaus, dass auch die Verbindung von Cybersicherheit mit militärischer Führung, organisationsbezogenen Prozessen und allgemeiner IT-Betriebsfähigkeit ein wesentliches Ausbildungsmerkmal darstellen kann [11]-[15]. Diese Unterschiede verdeutlichen, dass Cybersicherheitsausbildung in militärischen Kontexten nicht losgelöst von strategischen Rollenverständnissen betrachtet werden kann. Ob ein Ausbildungsmodell eher defensiv, operativ-unterstützend, nachrichtendienstlich oder offensiv geprägt ist, hängt wesentlich davon ab, welche Funktionen Cyberkräfte innerhalb der jeweiligen Streitkräfte erfüllen sollen.

Für das Projekt Bumblebee lässt sich aus diesem Vergleich ableiten, dass die Übernahme eines einzelnen nationalen Modells weder zweckmäßig noch notwendig erscheint. Vielmehr spricht die Analyse für die Entwicklung eines eigenständigen, modular aufgebauten und zielgruppenorientierten Ausbildungskonzepts, das sich an operativen Erstreaktions- und Unterstützungsrollen orientiert und zugleich auf institutionelle Anschlussfähigkeit achtet [11]-[34]. Die internationalen Beispiele zeigen übereinstimmend, dass erfolgreiche Modelle klare Rollenprofile, nachvollziehbare curriculare Strukturen und eine enge Verbindung von Fachwissen, praktischer Anwendung und organisatorischer Einbettung aufweisen. Für Bumblebee bedeutet dies, dass technische Grundlagen, Erkennungs- und Analysekompetenz, Kommunikations- und Eskalationslogiken sowie praxisnahe Übungsformate systematisch miteinander verbunden werden sollten. Weniger zielführend erscheint hingegen eine unmittelbare Orientierung an hochspezialisierten oder offensiv ausgerichteten Modellen, wie sie in einzelnen Staaten für andere Rollenprofile entwickelt wurden.

Insgesamt macht der internationale Vergleich deutlich, dass ein tragfähiges Ausbildungsprogramm für den militärischen Cyberbereich weder ausschließlich akademisch noch ausschließlich technikorientiert konzipiert sein sollte. Vielmehr bedarf es eines konzeptionell ausgewogenen Ansatzes, der technische Grundbefähigung, prozessuale Handlungssicherheit, institutionelle Einbettung und realitätsnahe Übungssystematik miteinander verknüpft. Für Bumblebee ergibt sich daraus die Notwendigkeit, ein Ausbildungsformat zu entwickeln, das auf einem grundlegenden operativen Kompetenzniveau ansetzt, heterogene Eingangsvoraussetzungen berücksichtigt und die Teilnehmenden nicht primär zu Spezialistinnen und Spezialisten ausbildet, sondern zur sicheren Wahrnehmung von Erkennungs-, Erstbewertungs-, Dokumentations- und Eskalationsaufgaben befähigt. Gerade darin liegt die zentrale Lehre aus dem internationalen Vergleich: Nicht die größtmögliche Spezialisierung, sondern die passgenaue curriculare Ausrichtung auf die tatsächlichen Handlungsanforderungen der Zielgruppe ist entscheidend für die Wirksamkeit militärischer Cybersicherheitsausbildung [11]-[34].

3.7 Relevante Standards und Rahmenwerke für die Cybersicherheitsausbildung

Die Ausbildung im Bereich der Cybersicherheit orientiert sich, insbesondere im militärischen Kontext, an einer Vielzahl international etablierter Standards, Frameworks und Best Practices. Diese Referenzsysteme definieren nicht nur technische Anforderungen an den Schutz von Informationssystemen, sondern auch organisatorische, prozessuale und governancebezogene Rahmenbedingungen für den Umgang mit Cyberrisiken und Sicherheitsvorfällen. Für die Konzeption eines militärischen Ausbildungsprogramms ist ihre Berücksichtigung deshalb von zentraler Bedeutung, weil sie eine fachlich belastbare Strukturierung von Lernzielen, Kompetenzprofilen und Ausbildungsinhalten ermöglichen. Standards und Rahmenwerke fungieren in diesem Zusammenhang nicht lediglich als normative Hintergrundfolie, sondern als konzeptionelle Bezugspunkte, mit deren Hilfe technische Maßnahmen, organisatorische Zuständigkeiten und institutionelle Handlungserfordernisse systematisch miteinander verknüpft werden können. Im militärischen Umfeld kommt hinzu, dass Cybersicherheitsausbildung nicht isoliert im Rahmen einzelner Organisationen betrachtet werden kann. Vielmehr ist sie häufig in Bündnisstrukturen, internationale Kooperationen und interoperable Einsatzkontexte eingebettet. Dadurch gewinnen neben allgemeinen Informationssicherheitsstandards auch spezifische militärische Standardisierungsmechanismen an Bedeutung. Ausbildungsprogramme müssen sich daher sowohl an allgemein anerkannten Modellen des Informationssicherheitsmanagements als auch an militärisch relevanten Prinzipien der Interoperabilität, Standardisierung und prozessualen Einheitlichkeit orientieren. Für das Projekt Bumblebee ist dies besonders relevant, da das angestrebte Ausbildungsprogramm nicht nur technische Basisfähigkeiten vermitteln, sondern zugleich einen strukturierten, organisationsbezogen anschlussfähigen und international anschlussfähigen Qualifikationsrahmen bereitstellen soll.

Im Folgenden werden jene Standards und Rahmenwerke dargestellt, die für die Entwicklung eines Ausbildungsprogramms im Projekt Bumblebee als besonders relevant erscheinen. Dazu zählen militärische Standardisierungsvereinbarungen der NATO, internationale Normen im Bereich des Informationssicherheitsmanagements, Frameworks für IT-Governance und Service Management sowie Kompetenz- und Wissensrahmen für Cybersicherheit. Gemeinsam bilden sie eine tragfähige Grundlage für die Entwicklung eines strukturierten Curriculums, das sich an international anerkannten Best Practices orientiert und zugleich den spezifischen Anforderungen des militärischen Cyberkontexts Rechnung trägt.

3.7.1 Militärische Standardisierungsvereinbarungen (STANAG)

Die Standardization Agreements (STANAGs) stellen einen zentralen Mechanismus der NATO zur Herstellung und Sicherung militärischer Interoperabilität dar. Aus NATO-Perspektive dient Standardisierung dazu, die für gemeinsame Operationen erforderliche Kompatibilität, Austauschbarkeit und gemeinsame Verwendbarkeit von Verfahren, Systemen, Ausrüstung und Begrifflichkeiten herzustellen. Interoperabilität wird dabei als die Fähigkeit verstanden, dass Streitkräfte unterschiedlicher Nationen kohärent, effektiv und effizient gemeinsam handeln können, um taktische, operative und strategische Ziele zu erreichen [35]. STANAGs sind in diesem Zusammenhang jene NATO-Standardisierungsdokumente, in denen Mitgliedstaaten ihre Übereinkunft festhalten, einen bestimmten Standard ganz oder teilweise, gegebenenfalls mit Vorbehalt, umzusetzen, um ein konkretes Interoperabilitätsanfordernis zu erfüllen [35][36].

Inhaltlich decken STANAGs ein breites Spektrum militärischer Handlungsfelder ab. Sie betreffen nicht nur technische Spezifikationen von Systemen und Ausrüstung, sondern auch operative Verfahren, administrative Abläufe, Kommunikationsstandards, Formate für den Informationsaustausch, logistische Prozesse sowie materielle Schnittstellen [35]. NATO verweist

in diesem Zusammenhang beispielhaft auf Standards für Luftbetankungsverfahren, für die Interoperabilität nationaler Kommunikationssysteme, für Munitionsgrößen und Sicherheitsregeln oder für Formate des Nachrichtendienst- und Informationsaustauschs [35]. Daraus wird deutlich, dass STANAGs nicht als rein technische Detailregelungen zu verstehen sind, sondern als organisationsübergreifende Referenzsysteme, die eine gemeinsame militärische Operations- und Unterstützungsfähigkeit absichern. Für den Cyberbereich ist dies besonders relevant, da auch hier technische Kompatibilität, einheitliche Begriffsverwendung, standardisierte Kommunikationswege und abgestimmte Melde- und Reaktionsprozesse Grundvoraussetzungen wirksamer multinationaler Zusammenarbeit sind [35][36].

Institutionell werden STANAGs im NATO-Standardisierungssystem entwickelt und promulgiert. Das NATO Standardization Office (NSO) koordiniert und administriert die Standardisierungsaktivitäten der Allianz und unterstützt dabei sowohl den Committee for Standardization (CS) als auch den Militärischen Ausschuss. Der CS ist das senior body der NATO für Standardisierungspolitik und arbeitet unter der Autorität des North Atlantic Council; seine Aufgabe besteht darin, Standardisierungspolitik innerhalb der Allianz zu steuern und dadurch zur Entwicklung interoperabler und kosteneffizienter militärischer Fähigkeiten beizutragen [36][37]. Das NSO veröffentlicht ratifizierte STANAGs und Allied Publications, verwaltet die zugehörige Dokumentationsbasis und unterstützt darüber hinaus die Einbindung von Standardisierung in die NATO Defence Planning Process [36]. Aus dieser institutionellen Einbettung wird ersichtlich, dass STANAGs nicht isolierte Fachdokumente darstellen, sondern Teil eines umfassenderen Steuerungs- und Fähigkeitsentwicklungsprozesses innerhalb der Allianz sind.

Für die militärische Cybersicherheitsausbildung ergibt sich daraus eine mehrfache Relevanz. Erstens schaffen STANAGs einen gemeinsamen Referenzrahmen für interoperable Verfahren, was gerade in multinationalen Einsatz- und Unterstützungsstrukturen wesentlich ist. Zweitens fördern sie ein einheitliches Verständnis von Rollen, Kommunikationswegen, Meldeverfahren und sicherheitsrelevanten Prozesslogiken, was für die Ausbildung von Personal im SOC-/NOC-nahen Umfeld von besonderer Bedeutung ist. Drittens machen sie deutlich, dass militärische Handlungsfähigkeit im Cyberraum nicht allein auf technischer Expertise beruht, sondern ebenso auf der Fähigkeit, innerhalb standardisierter Bündnisstrukturen zu agieren. Dies ist insbesondere dann relevant, wenn Cybervorfälle in multinationalen Lagen erkannt, gemeldet, bewertet und koordiniert bearbeitet werden müssen. STANAGs wirken damit nicht nur auf der Ebene technischer Kompatibilität, sondern auch auf der Ebene gemeinsamer Verfahren und institutioneller Anschlussfähigkeit [35][36].

Darüber hinaus ist hervorzuheben, dass STANAGs und die zugehörigen Allied Publications nach NATO-Angaben auch für Evaluierungs- und Zertifizierungsprozesse relevant sind. Sie bilden eine wesentliche Grundlage für das NATO Evaluation Programme und für die Zertifizierung von Einheiten, die etwa für die NATO Response Force vorgesehen sind [35]. Für die Ausbildung bedeutet dies, dass Standardisierung nicht nur eine abstrakte Planungs- oder Doktrinfunktion erfüllt, sondern unmittelbar mit der Frage verknüpft ist, ob militärische Kräfte im Bündniskontext als einsatz- und kooperationsfähig gelten können. Im Kontext des Projekts Bumblebee folgt daraus, dass STANAGs zwar kein pädagogisches Framework im engeren Sinne darstellen, jedoch einen unverzichtbaren militärischen Ordnungs- und Anschlussrahmen bilden. Ihre curriculare Relevanz liegt daher weniger in der vollständigen Vermittlung einzelner Standardisierungsdokumente als vielmehr in der Einbettung des Ausbildungsprogramms in die Prinzipien von Interoperabilität, Standardisierung, prozessualer Einheitlichkeit und multinationaler Verwendbarkeit [35][36].

3.7.2 ISO/IEC 27000-Serie

Die ISO/IEC-27000-Serie stellt einen der international bedeutendsten Referenzrahmen für Informationssicherheit, Cybersecurity und datenschutzbezogene Sicherheitsorganisation dar. Sie

wurde gemeinsam von ISO und IEC im Rahmen des Joint Technical Committee ISO/IEC JTC 1, dort insbesondere durch das Subcommittee 27 (SC 27) „Information security, cybersecurity and privacy protection“, entwickelt [38][85]. Bereits diese institutionelle Einbettung ist für die wissenschaftliche Einordnung bedeutsam, weil sie verdeutlicht, dass die Normenfamilie nicht als sektor- oder branchenspezifische Einzellösung konzipiert ist, sondern als international anschlussfähiger Standardisierungsrahmen für den Schutz von Informationen und informationsverarbeitenden Systemen in unterschiedlichsten organisatorischen Kontexten. ISO selbst beschreibt die 27000-Familie als Standardreihe, die Organisationen aller Größen und Sektoren dabei unterstützt, informationsbezogene Werte wie Finanzdaten, geistiges Eigentum, Personaldaten oder von Dritten anvertraute Informationen systematisch zu schützen [38].

Im Zentrum der Normenfamilie steht das Konzept des Information Security Management System (ISMS). Dieses verfolgt einen managementorientierten Ansatz, in dem Informationssicherheit nicht als isolierte technische Schutzmaßnahme, sondern als kontinuierlicher, organisationsweiter und risikobasierter Steuerungsprozess verstanden wird [38]. Die Grundidee eines ISMS besteht darin, Informationssicherheit dauerhaft in organisatorische Prozesse, Verantwortlichkeiten, Richtlinien und Verbesserungszyklen einzubetten. Damit unterscheidet sich die ISO/IEC-27000-Serie von rein technisch-operativen Sicherheitskatalogen: Sie adressiert nicht nur Schutzmaßnahmen im engeren Sinn, sondern die systematische Fähigkeit einer Organisation, Sicherheitsrisiken zu identifizieren, zu bewerten, zu behandeln und fortlaufend zu überwachen. Für die militärische Cybersicherheitsausbildung ist dies besonders relevant, da Sicherheitsvorfälle in militärischen Kontexten regelmäßig nicht nur technische, sondern zugleich organisatorische, prozessuale und führungsbezogene Implikationen aufweisen. Innerhalb der Normenfamilie nimmt ISO/IEC 27001 eine Schlüsselrolle ein, da sie die Anforderungen an ein Informationssicherheitsmanagementsystem definiert und damit den normativen Kern des Rahmens bildet [6][86]. ISO beschreibt 27001 als weltweit bekanntesten Standard für ISMS und hebt hervor, dass die Norm Organisationen dabei unterstützt, ein System zur Steuerung informationsbezogener Risiken aufzubauen, umzusetzen, aufrechtzuerhalten und fortlaufend zu verbessern [86]. Für Ausbildungsprogramme ist dies insofern bedeutsam, als ISO/IEC 27001 ein strukturiertes Verständnis dafür vermittelt, dass Informationssicherheit auf klaren Verantwortlichkeiten, dokumentierten Verfahren, Risikobetrachtung und kontinuierlicher Verbesserung beruht. In einem militärischen Ausbildungskontext kann diese Perspektive dazu beitragen, Teilnehmende nicht nur auf technische Reaktionshandlungen, sondern auch auf die regelgeleitete Einbettung solcher Handlungen in organisatorische Sicherheitsstrukturen vorzubereiten.

Ergänzt wird ISO/IEC 27001 durch weitere Normen der Familie, die spezifische Teilbereiche vertiefen und operationalisieren. Von besonderer Bedeutung ist hier ISO/IEC 27002, die Leitlinien für Informationssicherheitskontrollen bereitstellt und damit den anforderungsorientierten Rahmen von ISO/IEC 27001 um umsetzungsnahe Best Practices ergänzt [38]. Hinzu kommen unter anderem ISO/IEC 27005 für das Informationssicherheits-Risikomanagement sowie die Normenreihe ISO/IEC 27035 für das Management von Informationssicherheitsvorfällen, die einen strukturierten Ansatz zur Erkennung, Meldung, Bewertung und Behandlung sicherheitsrelevanter Ereignisse beschreibt [38][87]. Auch der Standard ISO/IEC 27032 ist in diesem Zusammenhang relevant, da er die Beziehungen zwischen Cybersecurity, Netzwerksicherheit, Internetsicherheit und dem Schutz kritischer Informationsinfrastrukturen erläutert und damit eine breitere konzeptionelle Einordnung cyberbezogener Fragestellungen ermöglicht [88]. Die Normenfamilie ist damit nicht als monolithisches Einzelwerk, sondern als modularer Referenzrahmen zu verstehen, der unterschiedliche sicherheitsrelevante Problemstellungen systematisch abdeckt.

Für die militärische Cybersicherheitsausbildung ergibt sich aus dieser Struktur ein erheblicher Mehrwert. Die ISO/IEC-27000-Serie bietet nicht nur ein gemeinsames Begriffs- und Strukturmodell,

sondern auch eine belastbare Grundlage, um technische Inhalte mit organisatorischen und prozessualen Anforderungen zu verbinden. In einem Ausbildungskonzept wie Bumblebee kann sie insbesondere dazu beitragen, Lernziele in den Bereichen Risikomanagement, Informationssicherheitsorganisation, Vorfallsbehandlung, Dokumentation, Kontrollmechanismen und kontinuierliche Verbesserung systematisch zu verankern. Dies ist gerade deshalb bedeutsam, weil Personal in SOC-/NOC-nahen Rollen nicht nur einzelne technische Auffälligkeiten erkennen, sondern Vorfälle auch in einen geregelten organisatorischen Zusammenhang einordnen und entlang definierter Prozesse weiterverarbeiten muss. Die ISO/IEC-27000-Familie stellt hierfür einen international anschlussfähigen Referenzrahmen bereit, der technisches Handeln mit Management- und Prozesslogik verbindet [38][85][86]. Darüber hinaus ist die gemeinsame Herausgeberschaft von ISO und IEC auch inhaltlich relevant. Sie verdeutlicht, dass Informationssicherheit und Cybersecurity nicht nur klassische Management- oder IT-Themen sind, sondern zugleich eng mit der elektrotechnischen, systemischen und infrastrukturellen Dimension moderner Informations- und Kommunikationstechnologien verbunden bleiben. Gerade in militärischen Kontexten, in denen digitale Systeme, Kommunikationsnetze und technisch-kritische Infrastrukturen eng verflochten sind, ist diese gemeinsame Perspektive von besonderem Wert. Sie macht deutlich, dass Sicherheitsanforderungen sowohl auf Managementebene als auch auf Ebene technischer Systeme, Schnittstellen und Kontrollen gedacht werden müssen. In diesem Sinne ist die ISO/IEC-27000-Serie für Bumblebee nicht nur als Sammlung einzelner Normen relevant, sondern als übergreifender Referenzrahmen für eine risikobasierte, prozessorientierte und institutionell anschlussfähige Cybersicherheitsausbildung [38][85][86]. Insgesamt lässt sich die ISO/IEC-27000-Familie damit als einer der tragenden internationalen Standardisierungsrahmen für die Konzeption eines militärischen Ausbildungsprogramms im Bereich Cybersicherheit einordnen. Ihr besonderer Nutzen liegt darin, dass sie technische Sicherheitsaspekte nicht isoliert behandelt, sondern in ein umfassenderes Verständnis von Management, Risiko, Kontrolle, Vorfallsbehandlung und kontinuierlicher Verbesserung einbettet. Für das Projekt Bumblebee bedeutet dies, dass die Normenfamilie nicht nur als theoretischer Hintergrund herangezogen werden sollte, sondern als strukturgebende Grundlage für die curriculare Entwicklung – insbesondere dort, wo technische Grundkompetenzen mit organisatorischer Handlungssicherheit und prozessualer Verlässlichkeit verbunden werden sollen [6][38][4][86][87].

3.7.3 ITIL

Die IT Infrastructure Library (ITIL) stellt einen international etablierten Referenzrahmen für das IT-Service-Management dar und wird gegenwärtig in der Version ITIL 4 als umfassendes Framework für digitale Produkte und Services beschrieben [39][89]. Im Unterschied zu Standards, die primär Anforderungen an Informationssicherheitsmanagement oder technische Sicherheitskontrollen formulieren, richtet sich ITIL auf die Frage, wie IT-bezogene Leistungen geplant, bereitgestellt, betrieben und fortlaufend verbessert werden können. Im Zentrum steht dabei nicht allein die technische Funktionsfähigkeit einzelner Systeme, sondern die wertorientierte Gestaltung und Steuerung von Services in organisationalen Kontexten. Für die Cybersicherheitsausbildung ist ITIL deshalb von besonderer Relevanz, weil Cybervorfälle und sicherheitsbezogene Maßnahmen in der Praxis regelmäßig in bestehende Betriebs-, Kommunikations- und Eskalationsprozesse eingebettet sind. ITIL liefert hierfür einen strukturierten Bezugsrahmen, mit dessen Hilfe sich technische Reaktionen auf sicherheitsrelevante Ereignisse in organisatorisch nachvollziehbare und wiederholbare Abläufe überführen lassen. Ein zentrales Merkmal von ITIL 4 ist das Service Value System (SVS), das nach offizieller Beschreibung die Komponenten und Aktivitäten zusammenführt, durch die eine Organisation fortlaufend Wert schaffen kann [39][89]. Zum SVS gehören insbesondere die guiding principles, governance, die service value chain, practices sowie das Element der continuous improvement [39]. Ergänzend beschreibt ITIL 4 die four dimensions of service management – also organizations and people, information and technology, partners and suppliers sowie value streams and processes – als jene Perspektiven, die bei der Gestaltung und

Steuerung von Services systematisch berücksichtigt werden müssen [39][89]. Aus wissenschaftlicher Sicht ist dieser Ansatz für die militärische Cybersicherheitsausbildung besonders anschlussfähig, weil er verdeutlicht, dass Sicherheitsvorfälle nicht ausschließlich als technische Einzelereignisse verstanden werden dürfen. Vielmehr entstehen und eskalieren sie in organisationalen Zusammenhängen, in denen Personal, Technologie, externe Abhängigkeiten und definierte Prozessketten eng miteinander verflochten sind. Gerade im militärischen Umfeld, in dem Kommunikationswege, Zuständigkeiten und Meldekette klar geregelt sein müssen, bietet ITIL damit eine nützliche Perspektive, um technische und organisatorische Anforderungen nicht getrennt, sondern integriert zu betrachten.

Für den Kontext der Cybersicherheitsausbildung ist ITIL vor allem deshalb relevant, weil es eine Reihe von management practices beschreibt, die unmittelbar an die Behandlung sicherheitsrelevanter Ereignisse anschließen. Von besonderer Bedeutung sind hier insbesondere Incident Management, Problem Management, Change Enablement, Service Request Management, Monitoring and Event Management, Service Level Management, Continual Improvement sowie Information Security Management [90]. Diese Practices strukturieren nicht nur den Umgang mit Störungen und Veränderungen in IT-gestützten Umgebungen, sondern schaffen auch ein Prozessverständnis dafür, wie technische Beobachtungen in betriebliche Entscheidungen und koordinierte Reaktionsabläufe überführt werden. Für ein militärisches Ausbildungsprogramm ist dies von erheblicher Bedeutung, da Personal in SOC-/NOC-nahen Rollen nicht nur sicherheitsrelevante Ereignisse erkennen, sondern diese auch innerhalb definierter Abläufe klassifizieren, priorisieren, dokumentieren, kommunizieren und an zuständige Stellen weiterleiten muss. ITIL unterstützt damit die Entwicklung eines Ausbildungsverständnisses, in dem Cybersecurity nicht ausschließlich als Abwehrtechnik, sondern als Bestandteil belastbarer Service- und Betriebsprozesse verstanden wird. Gerade die Practices Incident Management, Problem Management und Change Enablement sind für Bumblebee besonders anschlussfähig. Incident Management adressiert die strukturierte Bearbeitung von Störungen und sicherheitsrelevanten Ereignissen, Problem Management richtet den Blick auf zugrunde liegende Ursachen und auf die Reduktion wiederkehrender Vorfälle, während Change Enablement beschreibt, wie Änderungen an Systemen und Services kontrolliert geplant, umgesetzt und kommuniziert werden können [55]. In militärischen Cyberkontexten ist diese Unterscheidung von hoher Relevanz, da die reine Erkennung eines Vorfalls noch keine wirksame Reaktion sicherstellt. Erst wenn Vorfälle in definierte Incident- und Eskalationsprozesse eingebettet, mögliche Ursachen analysiert und Gegenmaßnahmen kontrolliert umgesetzt werden, entsteht organisationsbezogene Handlungssicherheit. ITIL trägt insofern dazu bei, zwischen operativer Erstreaktion, systematischer Ursachenbearbeitung und kontrollierter Veränderung von Systemzuständen zu unterscheiden. Dies ist insbesondere für Ausbildungsprogramme wichtig, die nicht primär hochspezialisierte Forensik oder offensive Fähigkeiten vermitteln, sondern Personal zur regelgeleiteten Wahrnehmung von Erstreaktions- und Unterstützungsaufgaben befähigen sollen. Ein weiterer wesentlicher Mehrwert von ITIL liegt in seinem Fokus auf continual improvement. ITIL 4 beschreibt kontinuierliche Verbesserung als zentrales Prinzip, durch das Organisationen ihre Services, Prozesse und Praktiken fortlaufend anpassen und weiterentwickeln können [39][89]. Für die Cybersicherheitsausbildung ist dies aus zwei Gründen relevant. Erstens unterliegen Bedrohungslagen, technische Infrastrukturen und organisatorische Anforderungen im Cyberbereich einer hohen Dynamik, sodass Ausbildungsprogramme regelmäßig überprüft und angepasst werden müssen. Zweitens betrifft kontinuierliche Verbesserung nicht nur das Curriculum selbst, sondern auch die Fähigkeit der Teilnehmenden, aus Vorfällen, Übungen und Abweichungen zu lernen und Prozesse entsprechend weiterzuentwickeln. ITIL bietet hierfür keinen rein technischen Maßnahmenkatalog, sondern ein prozessorientiertes Verbesserungsverständnis, das besonders gut zu Ausbildungsumgebungen passt, in denen Übungsergebnisse, Fehlermuster und Lessons Learned systematisch ausgewertet und in die Weiterentwicklung von Szenarien, Unterlagen und Abläufen zurückgeführt werden sollen.

Für das Projekt Bumblebee ergibt sich daraus, dass ITIL nicht als konkurrierendes Sicherheitsframework zu ISO/IEC 27001, dem NIST CSF oder den CIS Controls zu verstehen ist, sondern als prozess- und serviceorientierte Ergänzung dieser Referenzmodelle. Während andere Frameworks stärker auf Risikomanagement, Sicherheitskontrollen oder Cyberfunktionen fokussieren, liefert ITIL einen besonders geeigneten Bezugsrahmen für die organisatorische Einbettung sicherheitsrelevanter Handlungen. Dazu gehören insbesondere Meldewege, Eskalationslogiken, Verantwortlichkeitszuweisungen, Servicekontinuität, Dokumentationsanforderungen und Verbesserungsprozesse. Im Curriculum kann ITIL deshalb vor allem dort produktiv eingesetzt werden, wo die Verbindung zwischen technischer Ereigniserkennung und organisationaler Reaktionsfähigkeit vermittelt werden soll. In diesem Sinne ist ITIL für Bumblebee weniger als rein theoretischer Hintergrund relevant, sondern als strukturierender Rahmen für Incident Response, Kommunikationsprozesse, kontrollierte Veränderungen und kontinuierliche Verbesserung in einem militärischen Ausbildungs- und Übungskontext [8][39][89][90].

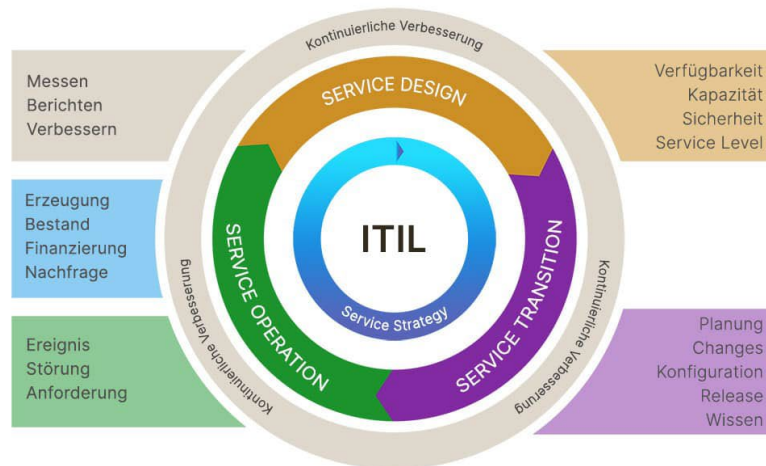


ABBILDUNG 1 ITIL V3 SERVICE LIFECYCLE (QUELLE: I-DOIT.COM)

3.7.4 COBIT

COBIT ist ein von ISACA entwickeltes Framework für die Governance und das Management von Enterprise Information and Technology (I&T). In seiner aktuellen Ausprägung als COBIT 2019 richtet sich das Framework nicht ausschließlich an IT-Abteilungen, sondern an die Gesamtorganisation und verfolgt das Ziel, durch eine wirksame Governance und Steuerung von Information und Technologie Wertschöpfung zu ermöglichen, Risiken zu steuern und Ressourcen zu optimieren [7][40]. Damit unterscheidet sich COBIT von stärker technisch oder operativ ausgerichteten Standards insofern, als der Schwerpunkt nicht primär auf einzelnen Sicherheitsmaßnahmen liegt, sondern auf der Frage, wie informations- und technologiebezogene Aktivitäten in strategische Zielsetzungen, Verantwortungsstrukturen und Kontrollmechanismen eingebettet werden können. Aus wissenschaftlicher Perspektive ist COBIT damit vor allem als Rahmenwerk der institutionellen Steuerung relevant, das Cybersicherheit nicht isoliert als technische Schutzfunktion, sondern als Bestandteil organisationaler Governance versteht.

Ein zentrales Merkmal von COBIT 2019 ist die klare Unterscheidung zwischen Governance und Management. In Übereinstimmung mit ISO/IEC 38500 beschreibt COBIT Governance als die Aufgabe, Stakeholder-Bedürfnisse, Rahmenbedingungen und Handlungsoptionen zu bewerten, Richtung vorzugeben und die Leistung sowie Compliance zu überwachen. Management wird demgegenüber als jene Tätigkeit verstanden, die auf Basis dieser Vorgaben plant, aufbaut, betreibt und überwacht, um die gesetzten Unternehmensziele zu erreichen [7][40][41]. Diese

Unterscheidung ist für die militärische Cybersicherheitsausbildung von besonderer Bedeutung, weil sie verdeutlicht, dass Sicherheitsentscheidungen nicht nur auf der operativen Ebene der Systemadministration oder Vorfallsbearbeitung stattfinden, sondern stets in übergeordnete Führungs-, Kontroll- und Verantwortungsstrukturen eingebettet sind. Gerade in militärischen Organisationen, in denen Zuständigkeiten, Rechenschaftspflichten und hierarchische Entscheidungswege eine zentrale Rolle spielen, bietet COBIT damit eine analytisch wertvolle Perspektive auf die institutionelle Verankerung von Cybersicherheit. Strukturell arbeitet COBIT 2019 mit einem Core Model aus 40 Governance- und Managementzielen, die auf fünf Domänen verteilt sind. Die Governance-Ziele sind im Bereich Evaluate, Direct and Monitor (EDM) gebündelt, während die Managementziele den Domänen Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS) sowie Monitor, Evaluate and Assess (MEA) zugeordnet werden [7][40]. Diese Struktur macht COBIT für Ausbildungszwecke besonders interessant, weil sie eine Brücke zwischen strategischer Steuerung und operativer Ausführung schlägt. Für ein militärisches Ausbildungsprogramm kann dies bedeuten, dass technische Inhalte wie Systembetrieb, Incident Handling oder Monitoring nicht isoliert betrachtet werden, sondern im Zusammenhang mit Planung, Verantwortlichkeitsverteilung, Serviceunterstützung und Evaluierung vermittelt werden. COBIT liefert damit kein Curriculum im engeren Sinn, wohl aber ein Ordnungsmodell, mit dessen Hilfe unterschiedliche Themenfelder der Cybersicherheit auf übergeordnete Organisations- und Steuerungszusammenhänge bezogen werden können.

Ein weiterer wesentlicher Aspekt von COBIT ist die Beschreibung der Governance-System-Komponenten. Nach ISACA umfasst COBIT 2019 dabei unter anderem Prozesse, Organisationsstrukturen, Prinzipien, Policies und Frameworks, Information, Kultur, Ethik und Verhalten, People, Skills and Competencies sowie Services, Infrastruktur und Anwendungen [40][41]. Diese Mehrdimensionalität ist aus didaktischer Sicht besonders wertvoll, da sie zeigt, dass Cybersicherheit nicht allein als technisches Problemfeld begriffen werden kann. Vielmehr hängen wirksame Sicherheitsstrukturen immer auch von Organisationskultur, Rollenverständnis, Qualifikation des Personals, dokumentierten Vorgaben und unterstützender Infrastruktur ab. Für die Entwicklung eines Ausbildungsprogramms wie Bumblebee ist dies insofern anschlussfähig, als hier ebenfalls nicht nur technische Kenntnisse vermittelt werden sollen, sondern auch prozessuale Handlungssicherheit, organisationsbezogene Orientierung und ein grundlegendes Verständnis für institutionelle Zuständigkeiten. COBIT unterstützt somit eine Ausbildungsperspektive, in der technische und organisatorische Dimensionen systematisch zusammengedacht werden.

Für die militärische Cybersicherheitsausbildung liegt der besondere Mehrwert von COBIT daher weniger in der Vermittlung konkreter Schutzmaßnahmen als vielmehr in der Rahmung von Cybersecurity als Governance- und Managementaufgabe. Das Framework hilft zu verdeutlichen, dass Sicherheitsvorfälle, Risiken und Schutzmaßnahmen nicht nur technisch erkannt und bearbeitet, sondern auch auf Ebene von Führung, Steuerung, Berichtswesen, Kontrolle und Ressourcenallokation adressiert werden müssen. Gerade in militärischen Kontexten, in denen Cybervorfälle Auswirkungen auf Führungsfähigkeit, Kommunikationssicherheit, Interoperabilität und Einsatzbereitschaft haben können, ist diese Perspektive von hoher Relevanz. Für Bumblebee kann COBIT deshalb insbesondere als ergänzender Bezugsrahmen dienen, um Themen wie Risikosteuerung, Verantwortlichkeitsverteilung, Kontrollmechanismen, Governance-Strukturen und Leistungsbewertung curricular einzuordnen. Anders als NIST CSF, ISO/IEC 27001 oder die CIS Controls ist COBIT nicht primär für die operative Vorfallsbearbeitung gedacht; gerade deshalb eignet es sich als komplementäres Framework, um die strategische und organisatorische Einbettung von Cybersicherheit im Ausbildungskontext sichtbar zu machen. Insgesamt lässt sich COBIT somit als ein Framework verstehen, das für das Projekt Bumblebee vor allem auf der Ebene der Governance, institutionellen Steuerung und organisatorischen Anschlussfähigkeit relevant ist. Es bietet eine strukturierte Perspektive darauf, wie Informations- und Technologieeinsatz so gestaltet werden kann, dass Sicherheitsziele nicht nur technisch, sondern auch organisatorisch

und strategisch unterstützt werden. Für die curriculare Entwicklung bedeutet dies, dass COBIT insbesondere dort berücksichtigt werden sollte, wo Lernende verstehen sollen, wie technische Beobachtungen, Sicherheitsmaßnahmen und Incident-Response-Aktivitäten in formale Verantwortungs-, Entscheidungs- und Kontrollstrukturen eingebettet sind. Damit ergänzt COBIT die stärker operativ und technisch ausgerichteten Frameworks um eine Perspektive, die für die nachhaltige institutionelle Verankerung militärischer Cybersicherheitskompetenz von wesentlicher Bedeutung ist [7][40][41].

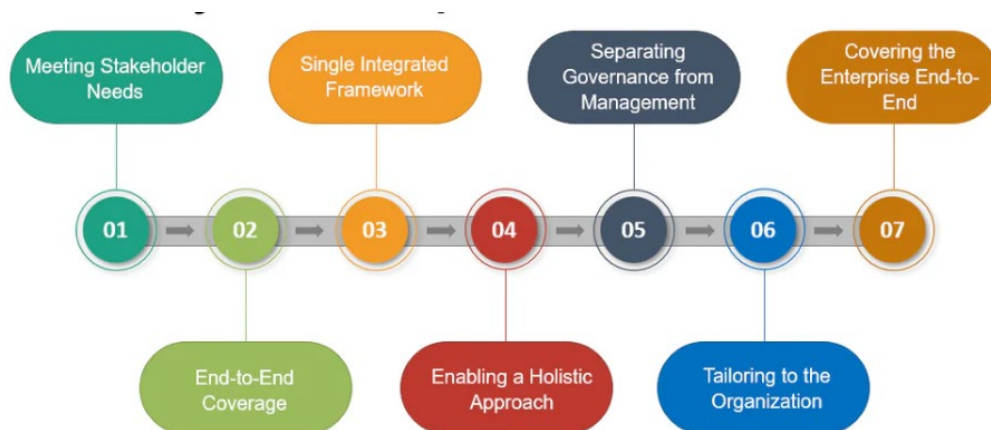


ABBILDUNG 2 COBIT SCHLÜSSELKOMponente (QUELLE: ITSM-DOCS.COM)

3.7.5 ENISA

Die European Union Agency for Cybersecurity (ENISA) nimmt innerhalb des europäischen Cybersicherheitsökosystems eine zentrale Rolle bei der Entwicklung von Kompetenzen, der Stärkung von Resilienz sowie der Unterstützung von Mitgliedstaaten und Organisationen im Umgang mit Cybervorfällen und Cyberkrisen ein. Im Unterschied zu klassischen Normungsorganisationen veröffentlicht ENISA keine formalen Standards im engeren Sinn, stellt jedoch praxisnahe Berichte, Methoden, Kompetenzrahmen, Good-Practice-Leitfäden und Unterstützungsinstrumente bereit, die für die Entwicklung von Ausbildungsprogrammen von erheblicher Relevanz sind. Besonders bedeutsam ist dabei, dass ENISA Cybersicherheit nicht nur als technisches Schutzproblem adressiert, sondern als Zusammenspiel aus Kompetenzen, Rollen, Organisation, Krisenmanagement und institutioneller Koordination versteht. Für die militärische Cybersicherheitsausbildung ist diese Perspektive deshalb besonders wertvoll, weil auch hier technische Fähigkeiten stets mit organisatorischen Verantwortlichkeiten, Kommunikationswegen, Eskalationslogiken und übergeordneten Resilienzanforderungen verknüpft sind.

Ein zentraler Beitrag von ENISA für die Curriculumentwicklung ist das European Cybersecurity Skills Framework (ECSF). ENISA beschreibt das ECSF als praktisches Instrument zur Identifikation und Strukturierung von Aufgaben, Kompetenzen, Skills und Wissensbeständen, die mit Rollenprofilen im Bereich Cybersicherheit verbunden sind. Zugleich wird es von ENISA ausdrücklich als EU-Referenzpunkt für die Definition und Bewertung relevanter Cybersecurity-Skills dargestellt. Das ECSF fasst den Cybersecurity-Arbeitsbereich in zwölf typische Rollenprofile zusammen und beschreibt für diese Rollen jeweils Verantwortlichkeiten, Aufgaben, erforderliche Kompetenzen, Skills, Wissensbereiche sowie Wechselwirkungen mit anderen Rollen [42][43]. Aus wissenschaftlicher Perspektive ist dieser Rahmen für Ausbildungsprogramme besonders anschlussfähig, weil er eine Abkehr von rein themen- oder technologiezentrierten Curricula ermöglicht und stattdessen eine rollen- und kompetenzorientierte Ausbildungslogik unterstützt. Für Bumblebee ist dies insofern besonders relevant, als das Projekt ebenfalls nicht auf eine unspezifische Vermittlung von Cyberwissen abzielt, sondern auf die strukturierte Befähigung von

Personal für klar umrissene operative Rollen im SOC-/NOC-nahen Umfeld. Das ECSF ist darüber hinaus nicht nur als deskriptives Rollenmodell bedeutsam, sondern auch als Instrument zur Harmonisierung von Ausbildung, Weiterbildung und Personalentwicklung. ENISA hebt hervor, dass das Framework eine gemeinsame Terminologie und ein gemeinsames Verständnis zwischen der Nachfrageseite – etwa Organisationen, Personalplanung und Rekrutierung – und der Angebotsseite – etwa Ausbildungs- und Qualifizierungsanbietern – schaffen soll. Gleichzeitig unterstützt es Lernanbieter bei der Entwicklung zielgerichteter Programme und hilft politischen Entscheidungsträgern dabei, Kompetenzlücken systematisch zu identifizieren und geeignete Maßnahmen zur Schließung dieser Lücken zu entwickeln [42][43]. Für ein militärisches Ausbildungsprogramm wie Bumblebee lässt sich daraus ableiten, dass ENISA nicht nur inhaltliche Orientierung bietet, sondern auch eine methodische Hilfestellung zur Ableitung von Lernzielen, Kompetenzprofilen und Qualifikationsniveaus. Gerade im Kontext heterogener Zielgruppen und unterschiedlicher Vorkenntnisse ist ein solcher rollenbasierter Referenzrahmen von besonderem Nutzen, weil er hilft, Ausbildungsinhalte nicht beliebig, sondern entlang funktional nachvollziehbarer Rollenanforderungen zu strukturieren. Neben der Kompetenz- und Rollenperspektive ist ENISA auch für den Bereich Cyber Incident Response und Cyber Crisis Management von hoher Relevanz. Nach eigenen Angaben unterstützt ENISA die Mitgliedstaaten, die Europäische Kommission und andere Akteure bei der Prävention und wirksamen Reaktion auf Cybersecurity-Incidents und Cyberkrisen. Dazu gehören unter anderem die Unterstützung der CSIRTs Network und der EU-CyCLONe, die Durchführung von Krisenübungen, Trainingsaktivitäten sowie Hilfestellungen für Mitgliedstaaten beim Aufbau von Krisenplänen und Krisenstrukturen [44]. Diese Tätigkeiten zeigen deutlich, dass ENISA Cybersicherheit nicht nur auf der Ebene technischer Schutzmaßnahmen adressiert, sondern auch auf der Ebene koordinierter Reaktion, operativer Lagebilderstellung, Informationsaustauschprozesse und strategischer Krisenbewältigung. Für die militärische Ausbildung ist dies insbesondere deshalb relevant, weil im militärischen Umfeld Vorfälle regelmäßig nicht isoliert bearbeitet werden, sondern in Kommunikations- und Eskalationsketten eingebunden sind, die klare Zuständigkeiten und abgestimmte Reaktionsmuster erfordern. ENISA bietet damit einen praxisnahen Bezugsrahmen für die curriculare Behandlung von Meldewegen, Rollenabgrenzung, Lageverständnis und abgestufter Reaktion auf Vorfälle und Krisen. Von besonderer Bedeutung für Ausbildungsprogramme ist außerdem, dass ENISA einen starken Fokus auf Übungen, Trainingsmethodik und Preparedness legt. Die Agentur organisiert seit Jahren groß angelegte europäische Cyberübungen und stellt auch Methoden bereit, mit denen Organisationen eigene Cybersecurity-Übungen entwickeln können. Dieser Übungsbezug ist für Bumblebee besonders anschlussfähig, da das Projekt gerade auf praxisnahe Ausbildung, realitätsnahe Szenarien und die Entwicklung operativer Handlungssicherheit ausgerichtet ist. ENISA liefert hier keine militärspezifische Doktrin, wohl aber einen wertvollen europäischen Referenzrahmen für die Frage, wie Fähigkeiten durch Übungen aufgebaut, überprüft und weiterentwickelt werden können. Die Verbindung von Rollenverständnis, Incident Response, Krisenmanagement und Übungslogik macht ENISA damit zu einem besonders geeigneten Rahmenwerk für die didaktische und organisatorische Ausgestaltung eines Cybersecurity-Ausbildungsprogramms.

Für das Projekt Bumblebee ergibt sich daraus, dass ENISA vor allem in zweifacher Hinsicht relevant ist. Erstens bietet das ECSF einen tragfähigen Rahmen zur rollen- und kompetenzorientierten Strukturierung des Curriculums. Zweitens liefern die ENISA-Aktivitäten im Bereich Incident Response, Krisenmanagement und Übungen wichtige Anknüpfungspunkte für die Ausgestaltung praxisnaher Trainings- und Eskalationsszenarien. Im Unterschied zu stärker normativen oder kontrollorientierten Frameworks wie ISO/IEC 27001 oder den CIS Controls liegt die besondere Stärke von ENISA somit in der Verbindung von Kompetenzrahmen, Rollenlogik, Krisenvorbereitung und praktischer Umsetzbarkeit. Für die Curriculumsentwicklung bedeutet dies, dass ENISA nicht lediglich als ergänzende europäische Quelle behandelt werden sollte, sondern als zentraler Bezugsrahmen für die Frage, welche Rollen ausgebildet werden sollen, welche

Kompetenzen diesen Rollen zuzuordnen sind und wie diese Kompetenzen in Übungs- und Reaktionskontexte überführt werden können [42][43][44].

3.7.6 NIST Cybersecurity Framework

Das NIST Cybersecurity Framework (CSF) gehört zu den international einflussreichsten und am weitesten verbreiteten Rahmenwerken zur Strukturierung von Cybersicherheitsrisiken und Sicherheitsmaßnahmen. In der aktuellen Version CSF 2.0, veröffentlicht am 26. Februar 2024, beschreibt NIST das Framework ausdrücklich als Leitfaden für Industrie, Behörden und sonstige Organisationen aller Größen, Sektoren und Reifegrade, nicht mehr nur für Betreiber kritischer Infrastrukturen. Das Framework stellt dabei keine starre Vorgabe einzelner Technologien oder Kontrollen dar, sondern eine Taxonomie hochrangiger Cybersicherheitsziele und -ergebnisse, die Organisationen dabei unterstützen soll, ihre Cyberrisiken besser zu verstehen, zu bewerten, zu priorisieren und gegenüber internen wie externen Stakeholdern nachvollziehbar zu kommunizieren [45][46]. Diese Offenheit und sektorübergreifende Anwendbarkeit macht das NIST CSF auch für den militärischen Ausbildungskontext besonders anschlussfähig, weil es keine spezifische Organisationsform voraussetzt, zugleich aber eine klare Struktur für den Umgang mit Cyberrisiken bietet. Ein zentrales Merkmal des Frameworks ist seine Gliederung in die sechs Kernfunktionen Govern, Identify, Protect, Detect, Respond und Recover. Während die fünf Funktionen Identify, Protect, Detect, Respond und Recover bereits aus früheren Versionen bekannt sind, wurde mit CSF 2.0 die Funktion Govern ausdrücklich hervorgehoben und als neue eigenständige Kernfunktion verankert. NIST betont, dass damit insbesondere Fragen der Cyberrisikosteuerung, der Verantwortlichkeiten, der Strategie, der Policies und der übergeordneten Einbettung von Cybersicherheit in Organisationsführung und Enterprise Risk Management stärker in den Vordergrund rücken. Diese Erweiterung ist fachlich bedeutsam, weil sie den Blick von der operativen Schutz- und Reaktionslogik auf die vorgelagerte Ebene von Steuerung, Aufsicht und institutioneller Verantwortung lenkt [45][46]. Für militärische Ausbildungsprogramme ist dies besonders relevant, da Sicherheitsvorfälle auch dort nicht nur technische, sondern stets organisatorische, führungsbezogene und prozessuale Implikationen besitzen.

Die Stärke des NIST CSF liegt darin, dass es Cybersicherheit als lebenszyklusorientierten Risikomanagementprozess beschreibt. Die Funktion Identify adressiert das Verständnis von Assets, Geschäfts- beziehungsweise Missionskontext, Risiken und Abhängigkeiten; Protect fokussiert auf Schutzmaßnahmen und Kontrollen; Detect auf die rechtzeitige Erkennung anomaler oder sicherheitsrelevanter Ereignisse; Respond auf strukturierte Reaktionsmaßnahmen; und Recover auf Wiederherstellung und Resilienz nach Vorfällen. Durch die ergänzende Funktion Govern wird diese Abfolge in einen übergeordneten Rahmen von Leitung, Priorisierung und Verantwortungszuweisung eingebettet [45][46]. Für die Entwicklung eines Curriculums ist diese Struktur besonders wertvoll, weil Lernziele, Module und praktische Szenarien entlang dieser Funktionen systematisch angeordnet werden können. Ein Ausbildungsprogramm kann damit nicht nur einzelne technische Fähigkeiten vermitteln, sondern diese in einen zusammenhängenden Handlungszyklus einordnen, der vom Risikoverständnis über Prävention und Erkennung bis hin zu Reaktion und Wiederherstellung reicht.

Aus didaktischer Perspektive bietet das NIST CSF darüber hinaus den Vorteil, dass es bewusst nicht vorschreibt, wie bestimmte Ergebnisse erreicht werden müssen. Vielmehr verweist NIST darauf, dass das Framework mit anderen Normen, Kontrollen und Leitlinien kombinierbar ist und über sogenannte Informative References an weitere Dokumente anschließt. Damit eignet sich das CSF besonders gut als übergeordnetes Struktur- und Kommunikationsmodell, das mit anderen Referenzrahmen – etwa ISO/IEC 27001, ITIL, ENISA oder den CIS Controls – verbunden werden kann [45][46]. Für Bumblebee ist dies von erheblicher Bedeutung, weil das Projekt nicht auf die vollständige Übernahme eines einzelnen Frameworks abzielt, sondern auf die Entwicklung eines

kohärenten Ausbildungskonzepts, in dem unterschiedliche Standards komplementär genutzt werden. Das NIST CSF kann in diesem Zusammenhang als ordnender Rahmen dienen, innerhalb dessen technische, organisatorische und didaktische Elemente zusammengeführt werden. Besonders anschlussfähig ist das Framework für Ausbildungsprogramme im Bereich SOC-/NOC-naher Erstreaktionsrollen. So lassen sich etwa Inhalte zur System- und Assetkenntnis, zur Risikoeinordnung und zur Kenntnis kritischer Abhängigkeiten der Funktion Identify zuordnen, während Themen wie Basisschutzmaßnahmen, Zugriffskontrollen oder sichere Konfigurationen im Bereich Protect verortet werden können. Die Ausbildung in Log-Analyse, Monitoring und Anomalieerkennung lässt sich mit Detect verbinden; Meldewege, Eskalationsmechanismen, strukturierte Vorfallsbearbeitung und Kommunikationsprozesse entsprechen der Funktion Respond; und Fragen der Wiederherstellung, Nachbereitung und Lessons Learned können unter Recover behandelt werden. Die Funktion Govern schließlich bietet einen geeigneten Rahmen, um Verantwortlichkeiten, Policies, Berichtswesen und die Einbettung von Cybersecurity in institutionelle Entscheidungsstrukturen zu thematisieren [45][46]. Gerade diese klare funktionale Gliederung macht das Framework für die Curriculumsentwicklung besonders nutzbar, da es eine systematische Übersetzung abstrakter Cyberrisikologik in konkrete Ausbildungsbausteine ermöglicht.

Für das Projekt Bumblebee ergibt sich daraus, dass das NIST CSF besonders gut als übergeordnetes Strukturmodell für das Curriculum geeignet ist. Es erlaubt, technische Inhalte, organisatorische Verfahren, Rollenprofile und Evaluationslogiken entlang eines gemeinsamen Rahmens zu ordnen und dabei zugleich ausreichend flexibel zu bleiben, um militärische Besonderheiten zu berücksichtigen. Im Unterschied zu rein kontrollorientierten Katalogen oder stark managementfokussierten Frameworks verbindet das CSF strategische Steuerung, operative Sicherheit und Wiederherstellung in einer für Ausbildungskontexte gut anschlussfähigen Gesamtlogik. Für die curriculare Entwicklung bedeutet dies, dass das Framework nicht nur als theoretischer Hintergrund dienen sollte, sondern als didaktische Strukturierungshilfe für Lernziele, Module, Szenarien und Übungsformate. In diesem Sinne ist das NIST Cybersecurity Framework für Bumblebee besonders wertvoll, weil es eine international anschlussfähige, zugleich aber flexibel anpassbare Grundlage für die Entwicklung eines militärisch orientierten Ausbildungsprogramms im Bereich Cybersicherheit bereitstellt [45][46].



ABBILDUNG 3 NIST RAHMENWERK (QUELLE: NIST.GOV)

3.7.7 Cybersecurity Body of Knowledge

Der Cyber Security Body of Knowledge (CyBOK) stellt einen umfassenden und systematisch aufgebauten Wissensrahmen für das Fachgebiet der Cybersicherheit dar. Ziel des Projekts ist es, das in Forschung und Praxis vorhandene Wissen so zu konsolidieren, dass es als belastbare Grundlage für Ausbildung, Training, Kursentwicklung und berufliche Weiterbildung genutzt werden kann. Auf der offiziellen Projektseite wird CyBOK ausdrücklich als „a comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector“ beschrieben. Zugleich wird hervorgehoben, dass das Projekt darauf abzielt, Cybersicherheit stärker in die Reihe etablierter wissenschaftlicher Disziplinen einzuordnen, indem das Feld durch international anerkannte Expertinnen und Experten in strukturierter Form aufgearbeitet wird. Für die Entwicklung eines Ausbildungsprogramms ist dies besonders relevant, weil CyBOK nicht primär einzelne Maßnahmen oder Prozesse normiert, sondern eine fachliche Gesamtarchitektur des Cybersecurity-Wissens bereitstellt. In seiner Funktion unterscheidet sich CyBOK damit deutlich von Frameworks wie dem NIST Cybersecurity Framework, ISO/IEC 27001 oder den CIS Controls. Während diese stärker auf Risikomanagement, Governance, Kontrollen oder organisatorische Verfahren ausgerichtet sind, verfolgt CyBOK in erster Linie einen wissenssystematischen Ansatz. Im Zentrum steht die Frage, welche Konzepte, Methoden, Themenfelder und Zusammenhänge das Fachgebiet Cybersicherheit ausmachen und wie diese in kohärenter Form beschrieben werden können. Für die Curriculumentwicklung ist dies von besonderem Wert, da ein Ausbildungskonzept nicht nur operative Handlungen oder organisatorische Abläufe vermitteln muss, sondern auch auf einer nachvollziehbaren Auswahl und Strukturierung von Wissensbeständen beruhen sollte. CyBOK bietet hierfür einen Referenzrahmen, mit dem sich Ausbildungsinhalte fachlich verorten, voneinander abgrenzen und in einen größeren Gesamtzusammenhang einordnen lassen. Die aktuelle Wissensbasis von CyBOK liegt in Version 1.1 vor. Nach Angaben des Projekts wurde diese Version im Juli 2021 veröffentlicht und erweitert die vorherige Version 1.0 um zwei zusätzliche Knowledge Areas, nämlich Applied Cryptography und Formal Methods for Security. Darüber hinaus enthält Version 1.1 eine größere Überarbeitung des Bereichs Network Security, kleinere Anpassungen im Bereich Risk Management & Governance sowie einen umfangreichen Begriffsindex. Damit umfasst CyBOK in seiner aktuellen Fassung 21 Knowledge Areas, die als strukturierte Wissensgebiete den inhaltlichen Umfang des Fachgebiets Cybersicherheit abbilden. Für die wissenschaftliche Fundierung eines Curriculums ist dies besonders hilfreich, weil damit nicht nur einzelne Themen benannt, sondern deren Stellung innerhalb eines konsolidierten Wissenssystems nachvollziehbar gemacht werden kann.

Besonders relevant für Ausbildungszwecke ist die Art und Weise, wie CyBOK seine Wissensgebiete strukturiert. Bereits Version 1.0 gliederte die Knowledge Areas in mehrere übergeordnete Kategorien und machte zugleich deutlich, dass die einzelnen Wissensbereiche nicht orthogonal, also nicht streng voneinander getrennt, zu verstehen sind. Vielmehr bestehen zwischen ihnen vielfältige Beziehungen und Abhängigkeiten. Zusätzlich weist CyBOK explizit auf externe Wissensabhängigkeiten hin, etwa zu allgemeiner Informatik oder Software Engineering, und verknüpft einzelne Bereiche mit etablierten Referenzwerken wie SWEBOK oder dem ACM Curriculum. Diese Offenlegung von Zusammenhängen ist für die Curriculumentwicklung besonders bedeutsam, weil sie dabei hilft, Vorwissensanforderungen, Querverbindungen und die innere Logik eines Ausbildungsprogramms transparent zu machen. Gerade für Bumblebee, wo ein grundlegendes, aber systematisch aufgebautes Qualifikationsprofil angestrebt wird, bietet CyBOK damit eine tragfähige Grundlage zur Auswahl, Begrenzung und didaktischen Reihenfolge von Inhalten. Inhaltlich deckt CyBOK ein sehr breites Spektrum ab. Zu den Wissensbereichen gehören unter anderem Risk Management & Governance, Law & Regulation, Human Factors, Privacy & Online Rights, Malware & Attack Technologies, Adversarial Behaviours, Security Operations & Incident Management, Forensics, Cryptography, Operating Systems & Virtualisation Security, Distributed Systems Security, Authentication, Authorisation & Accountability, Software Security,

Web & Mobile Security, Secure Software Lifecycle, Network Security, Hardware Security, Cyber Physical Systems sowie Physical Layer and Telecommunications Security. Bereits diese Vielfalt macht deutlich, dass CyBOK Cybersicherheit nicht auf rein technische Schutzmaßnahmen reduziert, sondern auch organisatorische, menschliche, regulatorische und infrastrukturelle Dimensionen integriert. Für ein militärisches Ausbildungsprogramm ist dies besonders wertvoll, da auch dort operative Handlungssicherheit nur dann entstehen kann, wenn technische, organisatorische und kontextuelle Aspekte zusammengedacht werden.

Für das Projekt Bumblebee liegt der besondere Nutzen von CyBOK daher in seiner Funktion als fachlicher Ordnungsrahmen. Das Framework hilft dabei, die im Curriculum zu behandelnden Themen nicht allein aus einzelnen Bedarfsbeobachtungen oder aus der Logik spezifischer Tools abzuleiten, sondern sie in einen wissenschaftlich anschlussfähigen Gesamtzusammenhang einzubetten. So können etwa für ein grundlegendes operatives Ausbildungsprogramm gezielt jene Knowledge Areas ausgewählt werden, die für SOC-/NOC-nahe Erstreaktionsrollen besonders relevant sind, etwa Security Operations & Incident Management, Network Security, Authentication, Authorisation & Accountability, Risk Management & Governance, Malware & Attack Technologies oder Grundlagen aus Cryptography. CyBOK zwingt dabei nicht zur Übernahme des gesamten Wissensspektrums, sondern unterstützt gerade die reflektierte Auswahl jener Wissensbereiche, die für eine bestimmte Zielgruppe und ein bestimmtes Ausbildungsziel tatsächlich erforderlich sind. Hinzu kommt, dass CyBOK inzwischen nicht mehr nur aus dem Kernbestand der Knowledge Areas besteht, sondern auch durch Supplementary Guides ergänzt wird. Auf der offiziellen Projektseite wird erläutert, dass solche ergänzenden Guides insbesondere für emerging topics, weniger etablierte Themen oder anwendungsbezogene Querschnittsbereiche entwickelt werden. Dazu zählen Knowledge Guides und Topic Guides, etwa zu Security and Privacy of AI, Security Economics oder AI for Security. Diese Erweiterbarkeit ist aus curriculärer Sicht besonders interessant, weil sie zeigt, dass CyBOK nicht als statisches abgeschlossenes Werk verstanden werden sollte, sondern als weiterentwickelbarer Wissensrahmen, der auf neue Themen und Anwendungsfelder reagieren kann. Für Bumblebee bedeutet das, dass CyBOK nicht nur für die Definition eines Grundcurriculums nützlich ist, sondern auch als Referenz für die spätere Erweiterung um neue technologische oder operationelle Themenfelder dienen kann.

CyBOK lässt somit als ein wissenschaftlich orientierter, inhaltlich breit angelegter und für Ausbildungszwecke besonders geeigneter Wissensrahmen einordnen. Sein besonderer Wert liegt weniger in der direkten Steuerung von Sicherheitsmaßnahmen als in der systematischen Strukturierung des Fachwissens, auf dem Ausbildung, Training, Kursentwicklung und professionelle Weiterqualifizierung aufbauen können. Für das Projekt Bumblebee ist CyBOK daher insbesondere dort relevant, wo es darum geht, ein Curriculum fachlich zu fundieren, Themenfelder nachvollziehbar auszuwählen und zwischen grundlegenden und vertiefenden Inhalten zu unterscheiden. Im Zusammenspiel mit stärker prozess- und governanceorientierten Frameworks wie NIST, ISO/IEC, ITIL oder ENISA kann CyBOK die inhaltliche Wissensbasis bereitstellen, auf der ein militärisch anschlussfähiges und didaktisch kohärentes Ausbildungsprogramm aufbaut [47][48][49].

3.7.8 CIS Critical Security Controls

Die CIS Critical Security Controls stellen einen international verbreiteten, stark praxisorientierten Referenzrahmen für die Priorisierung und Umsetzung von Cybersicherheitsmaßnahmen dar. Nach offizieller Beschreibung des Center for Internet Security (CIS) handelt es sich um eine prescriptive, prioritized, and simplified set of best practices, die Organisationen dabei unterstützen soll, ihre Systeme und Daten gegen die häufigsten Angriffsvektoren zu schützen [10][84]. Im Unterschied zu stärker management- oder governanceorientierten Frameworks wie ISO/IEC 27001, ITIL oder COBIT liegt der Schwerpunkt der CIS Controls auf konkreten, operativ umsetzbaren

Schutzmaßnahmen. Für die militärische Cybersicherheitsausbildung ist dies besonders relevant, weil die Controls eine direkte Brücke zwischen abstrakten Sicherheitszielen und beobachtbaren, trainierbaren Handlungen schlagen. Sie eignen sich daher in besonderer Weise, um technische und organisatorische Mindestmaßnahmen in ein anwendungsnahes Ausbildungskonzept zu überführen. In der aktuellen Version v8.1 beschreibt CIS die Controls als priorisierte Menge von Safeguards, die auf die Abwehr der „most prevalent cyber attacks against systems and networks“ ausgerichtet sind [10]. CIS hebt hervor, dass v8.1 eine iterative Weiterentwicklung von v8 darstellt und unter anderem eine aktualisierte Ausrichtung auf veränderte Standards und Frameworks, überarbeitete Asset Classes, präzisere Safeguard-Beschreibungen sowie die Integration der Governance-Funktion in Anlehnung an NIST CSF 2.0 umfasst [84]. Diese Weiterentwicklung ist aus curriculärer Perspektive bedeutsam, weil sie zeigt, dass die Controls nicht als statischer Maßnahmenkatalog verstanden werden sollten, sondern als anpassungsfähiger Bezugsrahmen, der auf Veränderungen technologischer Umgebungen, hybrider Arbeitsformen und neuer Bedrohungsmuster reagiert. Gerade für Ausbildungsprogramme im militärischen Kontext ist diese Aktualisierungsfähigkeit wichtig, da auch dort Bedrohungslagen, Systemlandschaften und organisatorische Anforderungen fortlaufendem Wandel unterliegen. Ein zentrales Strukturmerkmal der CIS Controls ist ihre Organisation über Safeguards und Implementation Groups (IGs). CIS beschreibt die Implementation Groups als priorisierende Hilfestellung für Organisationen unterschiedlicher Größe, Komplexität und Risikolage. Dabei gilt IG1 als „essential cyber hygiene“ und wird ausdrücklich als Einstiegspunkt für alle Organisationen empfohlen; IG2 baut darauf auf, während IG3 die vollständige Tiefe des Modells mit zusätzlichen Maßnahmen für komplexere und stärker exponierte Umgebungen abbildet [84]. Nach den offiziellen CIS-Angaben umfassen v8 und v8.1 insgesamt 153 Safeguards, von denen 56 Safeguards der IG1 zugeordnet sind [84]. Für Ausbildungsprogramme ist diese Priorisierungslogik von besonderem Wert, weil sie eine gestufte didaktische Struktur nahelegt: Nicht alle Sicherheitsmaßnahmen müssen für jede Zielgruppe mit derselben Tiefe vermittelt werden; vielmehr kann entlang der Implementation Groups zwischen grundlegenden, erweiterten und spezialisierten Kompetenzanforderungen differenziert werden. Für Bumblebee ist dies besonders anschlussfähig, da das Projekt ebenfalls auf ein gestuftes Ausbildungskonzept für heterogene Zielgruppen abzielt.

Inhaltlich decken die CIS Controls ein breites, zugleich aber stark handlungsorientiertes Spektrum sicherheitsrelevanter Themen ab. Bereits die ersten Controls adressieren grundlegende Aufgaben wie Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management sowie Penetration Testing [56]. Diese Themenwahl ist für ein militärisches Ausbildungsprogramm besonders relevant, weil sie sich eng an jenen Tätigkeiten orientiert, die für die Überwachung, Absicherung, Dokumentation und Reaktion im operativen Betrieb von IT- und Kommunikationssystemen tatsächlich erforderlich sind. Im Unterschied zu rein abstrakten Ordnungsrahmen bieten die CIS Controls damit einen besonders guten Ausgangspunkt, um konkrete Ausbildungsinhalte und Übungsszenarien aus operativen Schutzanforderungen abzuleiten.

Aus didaktischer Sicht liegt die besondere Stärke der CIS Controls in ihrer Umsetzungsnähe. CIS betont selbst, dass die Safeguards jeweils „one thing“ verlangen und damit einen vereinfachten, handlungsorientierten Zugang zu Cybersicherheit ermöglichen [10]. Für die Curriculumsentwicklung bedeutet dies, dass sich viele Controls unmittelbar in beobachtbare Lernziele, praktische Aufgaben und evaluierbare Übungsformate übersetzen lassen. Themen wie Asset-Inventarisierung, Softwareübersicht, Log-Management, Monitoring,

Schwachstellenmanagement oder grundlegende Incident-Response-Abläufe können auf Basis der Controls nicht nur theoretisch vermittelt, sondern in praxisnahen Szenarien konkret trainiert werden. Gerade für ein Ausbildungsprogramm, das auf SOC-/NOC-nahe Erstreaktions- und Unterstützungsrollen abzielt, ist diese Handlungsorientierung besonders wertvoll, da die Zielgruppe weniger strategische Governance-Tiefe als vielmehr belastbare operative Basiskompetenzen benötigt.

Für das Projekt Bumblebee ergibt sich daraus, dass die CIS Controls vor allem als praxisnaher Referenzrahmen für technische und organisatorische Basisschutzmaßnahmen relevant sind. Während Frameworks wie ISO/IEC 27001, NIST CSF oder ENISA stärker auf Management, Risikostrukturierung, Rollenorientierung und Incident-Response-Gesamtlogiken fokussieren, liefern die CIS Controls konkrete Anhaltspunkte dafür, welche Maßnahmen eine Organisation auf operativer Ebene tatsächlich umsetzen und trainieren sollte. Für das Curriculum bedeutet dies, dass sich die Controls besonders gut eignen, um praxisbezogene Module zu Themen wie Asset Management, sichere Konfiguration, Authentisierung, Logging, Monitoring, Recovery, Malware-Abwehr und Incident Handling zu strukturieren. Zugleich erlaubt die Logik der Implementation Groups, diese Inhalte auf ein der Zielgruppe angemessenes Komplexitätsniveau zu begrenzen. In diesem Sinne sind die CIS Controls für Bumblebee weniger als umfassendes strategisches Rahmenwerk, sondern vor allem als operativer und didaktischer Anker für die Vermittlung umsetzungsnaher Cyberhygiene und Erstreaktionsfähigkeit von hoher Relevanz [10][84].

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards 101 2/5 102 4/5 103 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards 101 3/7 102 6/7 103 7/7	CONTROL 03 Data Protection 14 Safeguards 101 6/14 102 12/14 103 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards 101 7/12 102 11/12 103 12/12	CONTROL 05 Account Management 6 Safeguards 101 4/6 102 6/6 103 6/6	CONTROL 06 Access Control Management 8 Safeguards 101 5/8 102 7/8 103 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards 101 4/7 102 7/7 103 7/7	CONTROL 08 Audit Log Management 12 Safeguards 101 3/12 102 11/12 103 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards 101 2/7 102 6/7 103 7/7
CONTROL 10 Malware Defenses 7 Safeguards 101 3/7 102 7/7 103 7/7	CONTROL 11 Data Recovery 5 Safeguards 101 4/5 102 5/5 103 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards 101 1/8 102 7/8 103 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards 101 0/11 102 6/11 103 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards 101 8/9 102 9/9 103 9/9	CONTROL 15 Service Provider Management 7 Safeguards 101 1/7 102 4/7 103 7/7
CONTROL 16 Applications Software Security 14 Safeguards 101 0/14 102 11/14 103 14/14	CONTROL 17 Incident Response Management 9 Safeguards 101 3/9 102 8/9 103 9/9	CONTROL 18 Penetration Testing 6 Safeguards 101 0/5 102 3/5 103 5/5

ABBILDUNG 4 CIS CONTROLS (QUELLE: TRIPWIRE.COM)

3.8 Implikationen für das Projekt Bumblebee

Die in diesem Kapitel analysierten Standards und Rahmenwerke bilden in ihrer Gesamtheit eine wesentliche konzeptionelle Grundlage für die Entwicklung des Ausbildungsprogramms im Projekt Bumblebee. Dabei zeigt sich, dass kein einzelnes Framework die für den militärischen Ausbildungskontext relevanten Anforderungen vollständig abdecken kann. Vielmehr ergibt sich ein mehrschichtiger Bezugsrahmen, in dem unterschiedliche Perspektiven auf Cybersicherheit miteinander verbunden werden müssen: militärische Interoperabilität und Standardisierung, risikobasiertes Informationssicherheitsmanagement, prozessorientierte Service- und Betriebslogik, Governance und institutionelle Steuerung, rollen- und kompetenzbezogene Strukturierung sowie praxisnahe operative Sicherheitsmaßnahmen [5][6][7][8][10][42][45][47]. Für das Projekt Bumblebee folgt daraus, dass die curriculare Entwicklung nicht auf der Übernahme eines einzelnen Standards beruhen sollte, sondern auf der reflektierten Kombination mehrerer Referenzrahmen, die jeweils unterschiedliche, aber komplementäre Funktionen erfüllen.

Aus konzeptioneller Sicht spricht die Analyse insbesondere dafür, das Ausbildungsprogramm entlang einer klaren funktionalen und zugleich mehrdimensionalen Logik aufzubauen. Das NIST Cybersecurity Framework eignet sich hierbei in besonderer Weise als übergeordnetes Strukturmodell, da es mit den Funktionen Govern, Identify, Protect, Detect, Respond und Recover einen nachvollziehbaren Ordnungsrahmen für Lernziele, Module und Übungsszenarien bietet [45][46]. Diese Struktur erlaubt es, technische Inhalte, organisatorische Abläufe und Reaktionslogiken nicht isoliert zu behandeln, sondern als zusammenhängenden Handlungszyklus zu vermitteln. Für Bumblebee ist dies besonders relevant, weil das angestrebte Ausbildungsprofil nicht auf hochspezialisierte Einzelkompetenzen ausgerichtet ist, sondern auf die Befähigung zur sicheren Wahrnehmung operativer Erstreaktions- und Unterstützungsaufgaben im SOC-/NOC-nahen Umfeld. Das NIST CSF kann damit als curriculare Leitstruktur dienen, innerhalb derer spezifischere Inhalte aus anderen Frameworks systematisch verortet werden.

Die ISO/IEC-27000-Serie ergänzt diesen Ordnungsrahmen um eine risikobasierte und managementorientierte Perspektive auf Informationssicherheit. Für das Projekt ist dies vor allem deshalb bedeutsam, weil dadurch verdeutlicht wird, dass Cybersicherheit nicht nur aus Einzelmaßnahmen oder Werkzeugkenntnissen besteht, sondern in organisatorische Prozesse, dokumentierte Verantwortlichkeiten, kontinuierliche Verbesserung und formalisierte Vorfallsbehandlung eingebettet werden muss [6][38][51][52]. Für das Curriculum folgt daraus, dass zentrale Themen wie Risikoverständnis, Sicherheitsorganisation, Incident Handling und dokumentierte Abläufe nicht nur implizit mitgeführt, sondern explizit als Lerngegenstände behandelt werden sollten. Gerade in einem militärischen Umfeld, in dem Verfahren, Rollen und Nachvollziehbarkeit eine besondere Bedeutung besitzen, trägt die ISO/IEC-Perspektive dazu bei, technische Handlungskompetenz mit prozessualer und institutioneller Verlässlichkeit zu verbinden.

ITIL und COBIT erweitern diese Perspektive um die Dimension der organisatorischen Einbettung, Governance und Serviceorientierung. ITIL ist insbesondere für die Modellierung von Incident- und Eskalationsprozessen, Kommunikationswegen, Servicekontinuität und kontinuierlicher Verbesserung relevant, während COBIT eine strukturierte Perspektive auf Verantwortungszuweisung, Kontrollmechanismen und institutionelle Steuerung von Information und Technologie bietet [7][8][39][40][41]. Für Bumblebee bedeutet dies, dass das Ausbildungsprogramm nicht nur technische Reaktionsfähigkeit vermitteln sollte, sondern auch ein grundlegendes Verständnis dafür, wie Vorfälle in geregelte organisatorische Abläufe eingebettet sind, welche Stellen in welcher Form einzubeziehen sind und wie technische Beobachtungen in Entscheidungs- und Berichtszusammenhänge überführt werden. Daraus folgt, dass Meldewege, Rollenverständnisse, Eskalationslogiken und Dokumentationsanforderungen nicht als Randthemen, sondern als integrale Bestandteile des Curriculums behandelt werden sollten.

Eine besondere Bedeutung kommt im europäischen Kontext ENISA und dem European Cybersecurity Skills Framework (ECSF) zu. Diese Rahmenwerke liefern für Bumblebee vor allem deshalb einen hohen Mehrwert, weil sie eine rollen- und kompetenzorientierte Strukturierung ermöglichen [42][43][44]. Während andere Standards vor allem Prozesse, Kontrollen oder Sicherheitsziele definieren, unterstützt das ECSF die Ableitung konkreter Kompetenzprofile und damit die curriculare Übersetzung abstrakter Anforderungen in zielgruppengerechte Lernziele. Für das Projekt bedeutet dies, dass Ausbildungsinhalte nicht allein entlang technischer Themenfelder organisiert werden sollten, sondern entlang jener Fähigkeiten, die für die anvisierten Rollen tatsächlich erforderlich sind. Dies ist insbesondere vor dem Hintergrund der im Projekt identifizierten Zielgruppe relevant, deren Aufgabenprofil stärker auf Erkennung, Erstbewertung, Dokumentation und Weiterleitung als auf vertiefte Spezialanalyse ausgerichtet ist.

Der Cyber Security Body of Knowledge (CyBOK) und die CIS Controls ergänzen diese Rahmenwerke um zwei weitere, für die Curriculumentwicklung zentrale Perspektiven. CyBOK stellt einen wissenschaftlich fundierten Wissensrahmen bereit, mit dessen Hilfe Themenfelder systematisch ausgewählt, voneinander abgegrenzt und in eine fachlich nachvollziehbare Gesamtstruktur eingeordnet werden können [47][48][49]. Die CIS Controls liefern demgegenüber einen besonders praxisnahen Bezugspunkt für jene Basisschutzmaßnahmen und operativen Handlungen, die sich in konkrete Übungen, Anwendungsfälle und technische Trainingsszenarien übersetzen lassen [10][56][57][58]. Für Bumblebee folgt daraus, dass ein tragfähiges Curriculum sowohl auf einer fachlich kohärenten Wissensstruktur als auch auf umsetzungsnahen, beobachtbaren und trainierbaren Handlungen beruhen sollte. Gerade die Kombination von CyBOK als Wissensarchitektur und CIS Controls als operativer Umsetzungsperspektive erscheint geeignet, um ein Ausbildungsprogramm zu entwickeln, das zugleich wissenschaftlich anschlussfähig und praxisorientiert ist.

Schließlich ist auch die militärische Standardisierungsperspektive durch STANAGs für das Projekt von Bedeutung. Zwar stellen STANAGs kein pädagogisches Framework im engeren Sinne dar, sie definieren jedoch den interoperablen Handlungsrahmen, innerhalb dessen militärische Kräfte in multinationalen Kontexten agieren müssen [5][35][36]. Für Bumblebee bedeutet dies, dass das Curriculum nicht ausschließlich auf nationale Organisationsrealitäten ausgerichtet werden sollte, sondern auch Prinzipien der Interoperabilität, Standardisierung und prozessualen Einheitlichkeit berücksichtigen muss. Dies betrifft insbesondere Terminologien, Kommunikationslogiken, standardisierte Melde- und Austauschprozesse sowie das Verständnis dafür, dass Cybervorfälle in militärischen Kontexten häufig nicht nur organisationsintern, sondern in übergeordneten Kooperations- und Bündnisstrukturen relevant werden.

Insgesamt ergibt sich daraus für das Projekt Bumblebee die Notwendigkeit eines mehrschichtigen curricularen Referenzmodells. Ein solches Modell sollte das NIST CSF als funktionale Grundstruktur nutzen, ISO/IEC-Normen für Risikomanagement und Vorfallsbehandlung heranziehen, ITIL und COBIT zur Vermittlung organisatorischer und governancebezogener Perspektiven einbeziehen, ENISA und das ECSF für Rollen- und Kompetenzprofile verwenden, CyBOK zur inhaltlichen Wissensstrukturierung nutzen und die CIS Controls als praxisnahen Anker für operative Schutz- und Reaktionsmaßnahmen heranziehen [5][6][7][8][10][42][45][47]. Die curriculare Konsequenz daraus ist eindeutig: Das Ausbildungsprogramm sollte nicht als Sammlung einzelner Themen oder Werkzeuge konzipiert werden, sondern als integriertes Qualifizierungssystem, das technische Grundlagen, organisatorische Prozesskompetenz, institutionelle Einbettung und praxisnahe Übungsfähigkeit systematisch miteinander verbindet. Gerade in dieser integrativen Verbindung liegt die zentrale Implikation der analysierten Standards und Frameworks für die weitere konzeptionelle Ausarbeitung von Bumblebee.

3.9 Trainingsplattformen und Cyber-Range-Umgebungen

Für die Ausbildung im Bereich der Cybersicherheit kommt praxisnahen Trainingsumgebungen eine zentrale Bedeutung zu. Während theoretische Inhalte die konzeptionelle und fachliche Grundlage schaffen, entsteht operative Handlungsfähigkeit erst durch die wiederholte Anwendung in kontrollierten, technisch belastbaren und didaktisch strukturierten Übungssettings. Trainingsplattformen und Cyber Ranges ermöglichen es, reale oder realitätsnahe Angriffsszenarien unter sicheren Bedingungen nachzubilden und dadurch sowohl technische als auch organisatorische Kompetenzen systematisch aufzubauen. Im militärischen Kontext ist dies von besonderer Relevanz, da hier nicht nur Einzelkompetenzen, sondern auch Teamarbeit, Meldekette, Reaktionsprozesse, Lagebildarbeit und Entscheidungsfindung unter Zeitdruck trainiert werden müssen [50][51]. Damit unterscheiden sich cyberbezogene Trainingsumgebungen grundlegend von rein theoretischen Lehrformaten: Sie dienen nicht nur der Wissensvermittlung, sondern der Einübung von Handlungsabläufen in einem sozio-technischen Kontext.

Eine Trainingsplattform im Bereich der Cybersicherheit kann allgemein als virtuelle oder softwaregestützte Umgebung verstanden werden, die für Schulung, Übung und Evaluierung eingesetzt wird. Sie stellt typischerweise Lerninhalte, technische Werkzeuge, Laborumgebungen, Simulationen und Übungsformate bereit, mit denen Teilnehmende ihr Wissen praktisch anwenden können. Solche Plattformen reichen von einfachen webbasierten Lernsystemen mit integrierten Aufgaben bis hin zu komplexen Umgebungen, in denen vollständige IT- oder OT-Infrastrukturen emuliert oder simuliert werden [52]. Ein verbreiteter didaktischer Ansatz innerhalb solcher Plattformen ist das Format Capture the Flag (CTF). Dabei bearbeiten Einzelpersonen oder Teams sicherheitsrelevante Aufgaben in einem zeitlich begrenzten Wettbewerbs- oder Übungsrahmen. Solche Formate fördern technisches Problemlösen, analytisches Denken und den Umgang mit typischen Sicherheitsproblemen. Für grundlegende und mittlere Ausbildungsstufen eignen sie sich besonders gut, da sie einen niederschweligen Einstieg in technische Sicherheitsfragen ermöglichen und gleichzeitig motivierend wirken können [53]. Für militärische Ausbildungsziele reichen sie allein jedoch in der Regel nicht aus, da dort zusätzlich organisationsbezogene Abläufe, Kommunikation, Rollenverteilung und Eskalationslogiken berücksichtigt werden müssen.

3.9.1 Trainingsplattformen für die Cybersicherheitsausbildung

Im Bereich der allgemeinen Cybersicherheitsausbildung existiert bereits eine Vielzahl etablierter Trainingsplattformen, die sich hinsichtlich Zielgruppe, didaktischer Struktur, technischer Tiefe und Anpassbarkeit deutlich unterscheiden. Für die Entwicklung eines militärisch anschlussfähigen Ausbildungskonzepts ist ihre Analyse insofern relevant, als sich an ihnen exemplarisch zeigen lässt, welche Lernformen sich für den Aufbau technischer Basiskompetenzen eignen und an welchen Punkten allgemeine Trainingsplattformen an Grenzen stoßen, wenn organisationsbezogene Abläufe, Rollenlogiken und kooperative Reaktionsszenarien vermittelt werden sollen. Besonders bedeutsam sind in diesem Zusammenhang Plattformen wie Hack The Box [54], TryHackMe [55], CTFd [56] und picoCTF [57], da sie unterschiedliche didaktische Paradigmen repräsentieren – von hochgradig praxisorientierten Angriffslaboren über geführte Lernpfade bis hin zu frei konfigurierbaren CTF-Umgebungen und stark einsteigerorientierten Schulungsformaten.

Hack The Box [54] ist eine Plattform, die sich stark an realitätsnahen technischen Szenarien orientiert und nach eigenen Angaben sowohl für Einzelpersonen als auch für Organisationen „real-world scenarios“, „gamified labs“ und „live-fire simulations“ bereitstellt. Offizielle Angaben verweisen auf Hunderte bis Tausende Labs, eine große internationale Community sowie auf role-based paths und spezielle Inhalte für SOC-, Pentest-, Cloud- und Blue-Team-Rollen. Besonders hervorzuheben ist, dass Hack The Box im Enterprise-Kontext nicht nur Einzelchallenges, sondern

auch Professional Labs mit mehrstufigen Unternehmensnetzwerken, realistischen Angriffspfaden und leistungsbezogenen Analysen anbietet [54]. Für die Ausbildung ist dies didaktisch relevant, weil damit nicht nur punktuell Aufgaben gelöst werden, sondern auch das Arbeiten in komplexeren, stärker zusammenhängenden Infrastrukturen unterstützt wird. Aus curriculärer Sicht eignet sich die Plattform deshalb vor allem für fortgeschrittene Ausbildungsphasen oder für Teilnehmende mit bereits vorhandenen technischen Grundlagen. Für Zielgruppen mit geringem Vorwissen kann der hohe technische Anspruch hingegen eine Hürde darstellen, wenn keine vorgelagerte Strukturierung oder tutorielle Begleitung vorgesehen ist.

TryHackMe [55] verfolgt demgegenüber einen stärker didaktisch geführten und einsteigerfreundlichen Ansatz. Die Plattform strukturiert Inhalte in Learning Paths, die Grundlagen- und Vertiefungsmodule mit praktischen Labs verbinden. Offizielle Lernpfade wie Pre Security, Cyber Security 101, SOC Level 1 oder SOC Level 2 zeigen, dass TryHackMe nicht nur technische Einzelthemen abbildet, sondern bewusst schrittweise Kompetenzentwicklung unterstützt – von Basiswissen zu Netzwerken, Linux, Windows und Kryptografie bis hin zu SIEM-Nutzung, Threat Detection, Incident Response und Threat Hunting [55]. Hinzu kommt, dass die Plattform für Teams die Erstellung und Anpassung eigener Lernpfade erlaubt, wodurch Inhalte zielgruppenspezifisch sequenziert und organisatorisch gesteuert werden können [55]. Für die Bedarfe des Projekts Bumblebee ist dies besonders anschlussfähig, da die empirische Analyse gezeigt hat, dass die Zielgruppe heterogene Eingangsvoraussetzungen aufweist. TryHackMe erscheint daher besonders geeignet für ein gestuftes Grundlagentraining, in dem technische Einführung, erste Tool-Nutzung und geführte Anwendungsszenarien systematisch miteinander verbunden werden. Weniger stark ausgeprägt ist allerdings die Abbildung komplexer organisationsbezogener Team- und Eskalationslogiken, wie sie für militärische Reaktionsszenarien erforderlich sein können.

CTFd [56] nimmt innerhalb dieses Vergleichs eine besondere Stellung ein, da es weniger eine inhaltlich vorkonfigurierte Lernplattform als vielmehr eine technische Grundlage zur Durchführung eigener CTF-Formate darstellt. Nach offizieller Beschreibung ist CTFd freie Open-Source-Software, die die Erstellung eigener Challenges, Docker-basierter Aufgaben, Benutzerverwaltung, Fortschrittsvisualisierung, Scoreboards sowie die Erweiterung über Themes und Plugins unterstützt [56]. Zusätzlich erlauben die offiziellen Dokumentationen die Implementierung eigener Challenge-Typen über Plugins, was die Plattform in didaktischer und technischer Hinsicht sehr flexibel macht [56]. Für Bumblebee ist CTFd daher insbesondere dort relevant, wo eigene, auf den militärischen Kontext zugeschnittene Aufgabenformate entwickelt werden sollen. Die Plattform eignet sich beispielsweise für die Durchführung kuratierter Grundlagenübungen, strukturierter Wettbewerbsszenarien oder prüfungsnaher Challenge-Formate. Ihr Vorteil liegt in der hohen Anpassbarkeit; ihr Nachteil besteht darin, dass sie ohne ergänzende didaktische Konzeption noch kein Curriculum im engeren Sinne bereitstellt. CTFd ist damit vor allem ein didaktisch formbares Trägersystem, dessen Qualität stark von der konkreten Szenario- und Aufgabenentwicklung abhängt.

picoCTF [57] ist deutlich stärker auf niederschwellige, einsteigerorientierte und bildungsnahe Zugänge ausgerichtet. Die Plattform wird von Carnegie Mellon University getragen und beschreibt sich selbst als kostenloses, spielerisches Bildungsprogramm, das Lernen, Üben und Wettbewerb im CTF-Format verbindet. Mit Angeboten wie dem picoGym und dem picoPrimer ermöglicht picoCTF sowohl nicht-kompetitive Übungsformen als auch klassische Wettbewerbsformate [57]. Offizielle Angaben von CMU betonen ausdrücklich, dass sich das Angebot an Lernende unterschiedlicher Erfahrungsstufen richtet und in einer sicheren Umgebung grundlegende bis fortgeschrittene Sicherheitsprinzipien vermittelt [57]. Für ein militärisches Ausbildungsprogramm ist picoCTF vor allem als Referenz für didaktisch stark geführte Grundlagenvermittlung interessant. Die Plattform zeigt, wie technische Sicherheitskonzepte über motivierende, niedrighschwellige und spielerische Aufgabenformate vermittelt werden können. Für die spezifischen Anforderungen von

Bumblebee – insbesondere mit Blick auf dokumentationsbezogene Abläufe, Meldewege, Teamkoordination und rollenbasierte Incident-Response-Szenarien – reicht picoCTF allerdings nicht aus. Ihr didaktischer Mehrwert liegt daher eher im Bereich des Vorkurs- oder Einstiegstrainings als in der Simulation operativer militärischer Handlungsfähigkeit.

Vergleichend lässt sich festhalten, dass die betrachteten Plattformen unterschiedliche Funktionen innerhalb eines mehrstufigen Ausbildungssystems erfüllen können. Hack The Box [54] eignet sich besonders für realitätsnahe, technisch anspruchsvolle und rollenbezogene Vertiefung, TryHackMe [55] für strukturierten Kompetenzaufbau und didaktisch geführte Lernpfade, CTFd [56] für die Entwicklung eigener challengebasierter Formate und picoCTF [57] für niederschwellige Grundlagenvermittlung und motivierende Einstiegsformate. Für die Konzeption eines militärischen Ausbildungsprogramms folgt daraus, dass keine dieser Plattformen für sich genommen sämtliche Anforderungen erfüllt. Vielmehr erscheint ein didaktisch kombinierter Einsatz sinnvoll, bei dem Grundlagen- und Tool-Kompetenzen zunächst über stärker geführte Lernumgebungen aufgebaut und anschließend durch individualisierte oder komplexere Szenarien vertieft werden. Für Bumblebee bedeutet dies insbesondere, dass allgemeine Trainingsplattformen zwar einen wichtigen Beitrag zum Aufbau technischer Basiskompetenzen leisten können, für die Ausbildung von Erstreaktion, Lagebildfähigkeit, Dokumentation, Kommunikationswegen und regelgeleiteter Eskalation jedoch durch spezifische Cyber-Range- oder organisationsorientierte Übungsformate ergänzt werden müssen [54][55][56][57].

3.9.2 Cyber Ranges als spezialisierte Trainingsumgebungen

Während allgemeine Trainingsplattformen vor allem auf die Vermittlung einzelner technischer Fertigkeiten, Aufgabenformate oder geführter Lernpfade ausgerichtet sind, gehen Cyber Ranges in ihrer Funktion deutlich darüber hinaus. Sie stellen spezialisierte Übungsumgebungen dar, in denen technische Systeme, Netzwerkstrukturen, Angriffs- und Verteidigungsszenarien sowie organisatorische Reaktionsabläufe in einer kontrollierten, isolierten und realitätsnahen Umgebung nachgebildet werden. NIST beschreibt einen Cyber Range in seinem Glossar als eine sichere, also sandboxartige Umgebung, in der praxisnahe Trainings, Szenarien, Challenges und Übungen durchgeführt werden können [76]. Diese Definition macht deutlich, dass Cyber Ranges nicht nur als technische Laborumgebungen, sondern als strukturierte Lern- und Übungsräume zu verstehen sind, in denen realitätsnahe Handlungsfähigkeit unter kontrollierten Bedingungen aufgebaut wird. Für die Cybersicherheitsausbildung ist dies von besonderer Bedeutung, weil sie einen Rahmen schaffen, in dem technisches Wissen nicht nur demonstriert, sondern in operative und oft zeitkritische Handlungssituationen überführt werden kann.

Im Unterschied zu einfacheren webbasierten Challenge-Plattformen zeichnen sich Cyber Ranges insbesondere durch ihren Systemcharakter aus. Sie bilden nicht bloß isolierte Aufgaben oder Einzelservices ab, sondern können ganze Netzwerksegmente, Serverlandschaften, Benutzerverhalten, Angriffsverläufe, Verteidigungsmaßnahmen und Kommunikationsketten integrieren. Dadurch eignen sie sich in besonderer Weise für Szenarien, in denen nicht nur Einzelpersonen, sondern Teams unter realitätsnahen Bedingungen zusammenarbeiten, Entscheidungen treffen und ihre Reaktionen koordinieren müssen. Diese Eigenschaft spiegelt sich auch in den von CISA angebotenen Cyber-Range-Trainings wider, die als interaktive, virtuelle und instruktionsgeleitete Formate mit praxisnahen Labs beschrieben werden. Dort werden insbesondere Fähigkeiten zur Untersuchung, Behebung und Reaktion auf Sicherheitsvorfälle in einer realistischen technischen Umgebung trainiert; die Angebote richten sich gezielt an Einsteiger- und mittlere Erfahrungsstufen und fokussieren auf technische Incident-Response-Kompetenzen [77]. Daraus wird ersichtlich, dass Cyber Ranges nicht nur für hochspezialisierte Expertinnen und Experten relevant sind, sondern bereits auf grundlegenden Ausbildungsniveaus ein wirksames

Instrument darstellen können, um technische und prozessuale Fähigkeiten handlungsorientiert zu vermitteln.

Aus didaktischer Perspektive liegt die besondere Stärke von Cyber Ranges darin, dass sie Realismus, Wiederholbarkeit und Sicherheit miteinander verbinden. Realismus ist dabei nicht als vollständige Abbildung operativer Realität zu verstehen, sondern als hinreichend plausible Nachbildung jener technischen und organisatorischen Bedingungen, unter denen sicherheitsrelevante Ereignisse auftreten und bearbeitet werden. Gleichzeitig müssen solche Umgebungen wiederholbar und kontrollierbar sein, damit Szenarien reproduziert, modifiziert und ausgewertet werden können. Genau diese Verbindung von realistischer Komplexität und didaktischer Steuerbarkeit unterscheidet Cyber Ranges von realen Produktionsumgebungen ebenso wie von stark abstrahierten Lernplattformen. Im europäischen Kontext unterstreicht ENISA die Relevanz solcher Trainings- und Übungsformate, indem die Agentur hervorhebt, dass Trainings und Exercises dazu dienen, Fähigkeiten aufzubauen, Lücken sichtbar zu machen und die Koordination in komplexen Cyberlagen zu verbessern. Das Programm Cyber Europe ist dabei explizit auf groß angelegte Vorfälle und Krisen vorbereitet und testet die Fähigkeit zur abgestimmten Reaktion über Organisations- und Ländergrenzen hinweg [78]. Für den militärischen Kontext ist dies besonders anschlussfähig, da auch dort technische Erkennung, operative Koordination, Kommunikationsdisziplin und abgestufte Eskalation gemeinsam trainiert werden müssen. Ein weiterer wesentlicher Unterschied zu einfachen Trainingsplattformen besteht darin, dass Cyber Ranges häufig mehrdimensionale Übungsziele unterstützen. In einer solchen Umgebung können nicht nur technische Analysen oder Verteidigungsmaßnahmen geübt werden, sondern auch Lagebilddarstellung, Berichtswesen, strategische Priorisierung, juristische Bewertung, mediale Reaktion oder Krisenkommunikation. Ein besonders prägnantes Beispiel hierfür ist die von der NATO CCDCOE organisierte Übung Locked Shields, die als jährliche Real-Time- bzw. Live-Fire-Cyberverteidigungsübung angelegt ist. Nach offizieller Beschreibung trainieren die teilnehmenden Teams dort nicht nur die Verteidigung nationaler IT-Systeme und kritischer Infrastrukturen unter laufenden Angriffen, sondern auch strategische Entscheidungsfindung, Forensik, rechtliche Bewertung, Medienarbeit und die Zusammenarbeit entlang der chain of command [79]. Neuere Beschreibungen betonen zusätzlich, dass sich die Übung über militärische, zivile, rechtliche und strategische Domänen erstreckt und dadurch gerade die Vielschichtigkeit realer Cybervorfälle abbildet [79]. Für die curriculare Ableitung ist dies besonders wichtig: Cyber Ranges sind dort am wertvollsten, wo Ausbildung nicht auf isolierte Tool-Kompetenz beschränkt bleibt, sondern die Verbindung von Technik, Kommunikation, Koordination und organisationsbezogener Reaktion einübt.

Technologisch beruhen Cyber Ranges dabei häufig auf einer Kombination aus Emulation, Simulation und Virtualisierung [59][60][61]. Emulation zielt darauf ab, reale Systeme und Dienste möglichst wirklichkeitsnah nachzubilden, während Simulation bestimmte Aspekte von Verhalten, Lasten oder Bedrohungsszenarien modellhaft abbildet. Virtualisierung schafft wiederum die technische Grundlage, um eine Vielzahl von Systemen, Netzen und Rollen effizient, isoliert und skalierbar bereitzustellen. Für die Ausbildung bedeutet dies, dass Cyber Ranges flexibel an unterschiedliche Zielsetzungen angepasst werden können: von technisch fokussierten Einzelübungen bis hin zu komplexen Team- und Krisenszenarien. Gerade im militärischen Bereich ist diese Flexibilität zentral, da Ausbildungsziele hier nicht nur technische Verteidigung, sondern ebenso Unterstützungsleistungen, Meldeprozesse, Führungszusammenhänge und die Einbindung in multinationale oder organisationsübergreifende Strukturen umfassen können. Cyber Ranges sind daher nicht bloß ein technisches Hilfsmittel, sondern ein eigenständiges didaktisches und infrastrukturelles Instrument, mit dem sich operative Cyberkompetenz systematisch entwickeln und evaluieren lässt [59][60][61][76][77][78][79].

Für das Projekt Bumblebee ergibt sich daraus, dass Cyber Ranges insbesondere dort relevant sind, wo über die Vermittlung von Grundlagenwissen hinaus realistische Erstreaktions-, Dokumentations-, Kommunikations- und Eskalationsszenarien trainiert werden sollen. Während klassische Lernplattformen und CTF-Formate vor allem für den Aufbau technischer Basiskompetenzen geeignet sind, bieten Cyber Ranges die Möglichkeit, diese Kompetenzen in komplexere sozio-technische Handlungszusammenhänge zu überführen. Damit stellen sie eine besonders geeignete Umgebung dar, um jene Fähigkeiten aufzubauen, die in der Bedarfserhebung als zentral identifiziert wurden: die Erkennung sicherheitsrelevanter Ereignisse, die strukturierte Erstbewertung, die Nachvollziehbarkeit von Meldungen und die organisationsbezogene Koordination von Reaktionen. Aus curriculärer Sicht sollten Cyber Ranges im Projekt daher nicht als isolierte Speziallösung verstanden werden, sondern als integraler Bestandteil eines gestuften Ausbildungsmodells, das technische Grundlagen mit realitätsnaher operativer Handlungssicherheit verbindet [59][60][61][77][79].

3.9.3 Beispiele bestehender Cyber Ranges

Die Betrachtung bestehender Cyber Ranges ist für das Projekt Bumblebee besonders aufschlussreich, weil sich an konkreten Umsetzungen erkennen lässt, welche funktionalen, didaktischen und infrastrukturellen Eigenschaften in der Praxis als relevant angesehen werden. Im Unterschied zu allgemeinen Trainingsplattformen zeigen diese Beispiele, wie Cyber Ranges reale oder realitätsnahe Infrastrukturen, organisationsbezogene Prozesse und unterschiedliche Zielgruppen in einem gemeinsamen Trainings- und Simulationsraum zusammenführen. Die hier betrachteten Systeme unterscheiden sich hinsichtlich Zielsetzung, technischer Architektur, Nutzerkreis und Einsatzbereich deutlich, weisen jedoch zugleich wiederkehrende Strukturmerkmale auf: hohe Anpassbarkeit, realistische Szenarien, Kombination aus Training und Testen, sowie die Möglichkeit, sowohl technische als auch organisatorische Fähigkeiten zu entwickeln. Gerade diese Mehrdimensionalität macht sie für die Ableitung eines militärisch anschlussfähigen Ausbildungsmodells besonders relevant.

Die DIATEAM Hybrid Cyber Range [62] steht exemplarisch für einen stark praxis- und anwendungsorientierten Ansatz. Nach offizieller Beschreibung ist sie als mobile, on-premise oder as-a-service bereitstellbare Plattform verfügbar und erlaubt die Nachbildung bestehender Informationssysteme, um Fähigkeiten wie Intrusion, Netzwerkschutz, Systemhärtung, Incident Response und TTP-basierte Trainings in anpassbaren Szenarien zu entwickeln. Besonders hervorzuheben ist die Möglichkeit, nicht nur klassische IT-, sondern auch OT-Komponenten und andere reale Netzwerkgeräte anzubinden, wodurch sich sektorübergreifende und cyber-physische Szenarien umsetzen lassen. Didaktisch relevant ist außerdem, dass der Komplexitätsgrad der Szenarien laut Anbieter von Einsteiger- bis Red-Team-Niveau moduliert werden kann. Damit repräsentiert DIATEAM ein Modell, bei dem technische Flexibilität, sektorale Anpassbarkeit und unterschiedlich tiefe Trainingspfade eng miteinander verbunden sind.

Die schwedische CRATE-Umgebung der FOI [63] repräsentiert demgegenüber einen besonders forschungsnahen und zugleich national sicherheitsbezogenen Cyber-Range-Ansatz. FOI beschreibt CRATE als eine der ersten und größten Cyber-Ranges Europas, mit der komplexe IT-Umgebungen einschließlich ICS-basierter kritischer Infrastrukturen unter kontrollierten Bedingungen aufgebaut und Angriffen ausgesetzt werden können. Die Plattform wird nicht nur für Übungen, sondern auch für Forschung zu Incident Management, Forensik, Angriffssimulation und Lernprozessen in hochqualifizierten Gruppen genutzt. Besonders bemerkenswert ist die cyber-physische Stadtmodellierung, die gesellschaftlich relevante Systeme wie Energieversorgung, Wasserwerke, Straßenverkehr und Eisenbahn in eine gemeinsame Trainingsumgebung integriert. Technisch verweist FOI auf mehr als 500 Virtualisierungsnodes, zwei getrennte Netzwerkzonen sowie einen hohen Grad an Automatisierung. CRATE steht damit für einen Range-Typ, bei dem

Forschung, großskalige technische Emulation und operative Übungsfähigkeit systematisch zusammengeführt werden.

Mit dem Realistic Global Cyber Environment (RGCE) von JYVSECTEC [64] liegt ein Beispiel für einen stark organisations- und kooperationsorientierten Range-Ansatz vor. Offizielle Angaben beschreiben RGCE als Finnlands nationale Cyber Range, die in einer isolierten Private-Cloud eine realistische globale Umwelt und reale Organisationsumgebungen zusammenführt. Hervorzuheben ist die große technische Breite: Die Plattform umfasst nach Anbieterangaben mehr als 7000 Systeme, Geräte und Services und bildet über 50 organisationsspezifische Umgebungen aus unterschiedlichen Sektoren ab, darunter kritische Infrastrukturen, Gesundheitswesen, Logistik, Regierung, Forschung und SOC-Umgebungen. Didaktisch besonders relevant ist, dass RGCE nicht nur technische Spezialisten adressiert, sondern ausdrücklich auch Management-Ebenen und die Zusammenarbeit mit Drittorganisationen und Dienstleistern einbezieht. Damit steht JYVSECTEC für einen Range-Ansatz, der technische Realitätsnähe mit sektoraler Vielfalt und interorganisationaler Koordination verbindet.

Die estnische Einrichtung CR14 [65] zeigt, wie ein Cyber Range in nationale Verteidigungsstrukturen und zugleich in NATO-nahe Zusammenhänge eingebettet werden kann. CR14 wurde laut eigener Darstellung vom estnischen Verteidigungsministerium gegründet, ist staatlich betrieben und bietet Cyber Ranges, Exercise Automation, eine digitale Bibliothek sowie Simulationswerkzeuge für Cyberverteidigungsaktivitäten an. Besonders wichtig ist die Angabe, dass CR14 zusätzlich Host Nation Support für das NATO CCDCOE leistet und seit Jahren den NATO Cyber Range mitentwickelt beziehungsweise betreibt. Die Plattform umfasst offene, nationale und NATO-bezogene Trainingsflächen sowie cyber-physische Lösungen wie Stromnetze, 5G-Netze, militärische Systeme und IoT. Damit verkörpert CR14 einen Range-Ansatz, der nationale Kompetenzentwicklung, internationale Kooperation und cyber-physische Erweiterbarkeit in einem politisch und militärisch hoch relevanten Rahmen zusammenführt.

Die Angebote von Leonardo [66] stehen exemplarisch für einen industriell geprägten und stark auf professionelle Einsatz- und Krisenszenarien ausgerichteten Ansatz. Leonardo beschreibt seine Cyber-Trainingslösungen als auf Virtualisierung, Emulation und Simulation basierende Umgebungen, mit denen flexible und dynamische Netzwerke für Übungen, Testbeds und komplexe Sicherheitsanalysen aufgebaut werden können. Ergänzend verweist Leonardo auf einen Cyber Trainer beziehungsweise X Range, der auf fortgeschrittenen Virtualisierungs-, KI- und Augmented-Reality-Technologien basiert und Teamtraining sowie Debriefing für komplexe Cyber-Warfare-Szenarien unterstützt. Die Beschreibung ist weniger akademisch als bei CRATE oder JYVSECTEC, zeigt aber deutlich, dass Leonardo Cyber Ranges als Teil eines professionellen Sicherheitsökosystems begreift, das SOC-/IOC-Unterstützung, Krisenreaktion, Training und technologische Integration miteinander verbindet. Für die vergleichende Betrachtung ist dies deshalb relevant, weil hier ein eher industrielles Modell sichtbar wird, das stark an Anwendbarkeit, Systemintegration und Einsatzunterstützung orientiert ist.

Die Norwegian Cyber Range [67], die an der NTNU verortet ist, verfolgt einen besonders breiten Ansatz, in dem Training, Testing, Exercises und Research ausdrücklich als gleichrangige Anwendungsfelder beschrieben werden. Nach offizieller Darstellung sollen Nutzer und Systeme dort in einer sicheren Umgebung realistischen Vorfällen ausgesetzt werden, um die Ausbildung und Übung von Sicherheitspersonal sowie die Erforschung und Erprobung neuer Lösungen zu unterstützen. Bemerkenswert ist die Betonung von gesellschaftlichen Funktionen und möglichen Kettenreaktionen, also eines Modells, bei dem nicht nur einzelne Organisationen, sondern je nach Szenario ganze Regionen oder nationale Zusammenhänge nachgebildet werden können. Damit repräsentiert der norwegische Ansatz einen Range-Typ, der stark auf Resilienzperspektiven, gesellschaftliche Verwundbarkeit und die Verbindung von Aus- und Weiterbildung mit Forschung und Systemtests ausgerichtet ist.

Cyberbit [68] schließlich steht exemplarisch für einen kommerziellen Range-Ansatz mit starker Fokussierung auf operative Einsatzreife. Laut Anbieter lassen sich realistische Range-Umgebungen innerhalb von Stunden bereitstellen; zentrale Merkmale sind die Nutzung realer Werkzeuge wie SIEMs, EDRs und Firewalls sowie Szenarien, die Entscheidungsfindung unter Zeitdruck fördern sollen. Cyberbit betont ausdrücklich, dass es nicht um das Erlernen einzelner Buttons, sondern um Handlungsfähigkeit unter realitätsnahen Angriffen geht. Damit ist Cyberbit besonders interessant für Ausbildungsziele, bei denen nicht primär die Infrastruktur selbst entwickelt werden soll, sondern eine schnell verfügbare, standardisierte und auf operative Verteidigung ausgerichtete Trainingsumgebung benötigt wird. Im Vergleich zu stärker forschungs- oder organisationsorientierten Plattformen ist hier die unmittelbare Umsetzbarkeit und Operationalisierung der Trainingsumgebung besonders stark ausgeprägt.

Die AIT Cyber Range [69] ist für das Projekt Bumblebee in besonderer Weise relevant, weil sie ein Beispiel für eine im deutschsprachigen Raum entwickelte Trainings- und Simulationsplattform darstellt, die ausdrücklich auf kritische IT- und OT-Infrastrukturen, Hands-on-Training, Incident Management und organisationale Resilienz ausgerichtet ist. Offizielle Angaben beschreiben die Plattform als virtuelle Umgebung für die flexible Simulation kritischer IT- und industrieller OT-Systeme mit komplexen Netzwerken, unterschiedlichen Systemkomponenten und Nutzerstrukturen. Sie wird laut AIT sowohl für Training, Exercises, Research als auch Development genutzt und adressiert unterschiedliche Zielgruppen – von Mitarbeitenden und IT-Professionals bis zu CERTs/CSIRTs, Management und Beiräten. Besonders hervorzuheben sind die enge Verbindung zur IAEA, die Durchführung nationaler Cyberübungen mit dem KSÖ seit 2017 sowie die explizite Ausrichtung auf kritische Infrastrukturen und OT-Sicherheit. Damit zeigt die AIT Cyber Range besonders deutlich, wie eine Range-Umgebung technische, organisatorische und strategische Zielgruppen in einem modularen Trainingsökosystem zusammenführen kann.

Vergleichend lässt sich damit festhalten, dass bestehende Cyber Ranges unterschiedliche Schwerpunkte setzen, sich jedoch in vier Typen gruppieren lassen: anwendungs- und kundenspezifische Hybrid-Ranges wie DIATEAM, forschungs- und verteidigungsnahe Großumgebungen wie CRATE oder CR14, organisations- und sektororientierte Resilienzplattformen wie JYVSECTEC oder AIT sowie kommerziell standardisierte Einsatzreife-Plattformen wie Cyberbit und Leonardo. Für das Projekt Bumblebee ist daraus abzuleiten, dass eine geeignete Range-Umgebung nicht nur technisch realistisch, sondern auch didaktisch modular, organisatorisch anschlussfähig und für unterschiedliche Kompetenzniveaus nutzbar sein sollte. Besonders relevant erscheinen dabei jene Merkmale, die mehrere der betrachteten Beispiele gemeinsam aufweisen: flexible Szenariokonfiguration, Integration von IT und OT, Unterstützung von Incident-Response- und Kommunikationsprozessen, Wiederverwendbarkeit der Infrastruktur sowie die Möglichkeit, sowohl Einzelpersonen als auch Teams und Führungsebenen in gemeinsame Übungslagen einzubinden [62]-[69].

3.9.4 Technologie-Stack von Cyber Ranges

Der technologische Aufbau von Cyber Ranges ist ein zentraler Faktor für ihre Funktionalität, Skalierbarkeit und didaktische Wirksamkeit. Im Unterschied zu einfachen webbasierten Trainingsplattformen, die sich häufig auf einzelne Aufgaben, isolierte Labs oder Challenge-Mechanismen beschränken, beruhen Cyber Ranges auf einer mehrschichtigen Infrastruktur, in der Rechenressourcen, Netzwerke, virtuelle Systeme, Automatisierung, Szenariosteuerung und Auswertungsmechanismen eng miteinander verzahnt sind. Ziel eines solchen Technologie-Stacks ist es, realitätsnahe, kontrollierbare und wiederholbare Übungsumgebungen bereitzustellen, in denen technische, organisatorische und gegebenenfalls auch führungsbezogene Reaktionen auf Cybervorfälle trainiert werden können. Aus architektonischer Sicht handelt es sich damit um komplexe soziotechnische Systeme, deren Wert nicht allein in der Bereitstellung technischer

Komponenten, sondern in deren orchestrierter Zusammenführung zu belastbaren Trainings- und Simulationsumgebungen liegt [70]. Für das Projekt Bumblebee ist diese Perspektive besonders relevant, weil sich daraus ableiten lässt, dass die Auswahl einer geeigneten Range-Technologie immer im Zusammenhang mit didaktischen Zielsetzungen, Rollenmodellen und organisatorischen Ausbildungsbedarfen betrachtet werden muss.

Die unterste Schicht eines solchen Stacks bildet in der Regel die Infrastrukturplattform, auf der virtuelle Maschinen, Container, Netzwerke und Speicherressourcen bereitgestellt werden. In vielen professionellen Cyber Ranges kommen dafür cloud- oder rechenzentrumsnahe Plattformen zum Einsatz, da diese eine flexible Zuteilung von Ressourcen, Mandantenfähigkeit, Netzwerksegmentierung und wiederholbare Szenariobereitstellung unterstützen. Ein typisches Beispiel ist OpenStack, das sich selbst als Open-Source-Cloud-Betriebssystem beschreibt, das große Pools von Rechen-, Speicher- und Netzwerkressourcen kontrolliert und über APIs oder Dashboards verwaltet [71]. Diese Charakteristik macht OpenStack für Cyber-Ranges besonders attraktiv, weil sich damit umfangreiche virtuelle Übungslandschaften mit getrennten Netzen, unterschiedlichen Rollenbereichen und definierter Zugriffskontrolle aufbauen lassen. Für militärische Ausbildungsszenarien ist dies von hoher Relevanz, da sich so abgeschlossene, kontrollierte und zugleich hochgradig anpassbare Übungsräume schaffen lassen, die unabhängig von produktiven Systemen betrieben werden können. Auf dieser Infrastruktur aufbauend kommen typischerweise Virtualisierungs- und Containerisierungstechnologien zum Einsatz. Virtuelle Maschinen eignen sich insbesondere für die Nachbildung vollständiger Betriebssysteme, komplexer Netzwerksegmente oder voneinander isolierter Zielsysteme. Containerbasierte Technologien bieten demgegenüber Vorteile in Bezug auf Portabilität, Ressourceneffizienz und Wiederholbarkeit. Docker beschreibt Container als isolierte Prozesse mit eigenen Dateisystemen, Netzwerken und Konfigurationsumgebungen, die sich dadurch besonders gut für standardisierte und reproduzierbare Deployment-Szenarien eignen [72]. Für Cyber Ranges ist diese Trennung didaktisch bedeutsam: Während virtuelle Maschinen vor allem für realitätsnahe Zielsysteme, Active-Directory-Strukturen oder persistente Netzwerkkontexte geeignet sind, können Container besonders effizient für kurzlebige Dienste, standardisierte Angriffs- oder Analysewerkzeuge und elastisch skalierbare Szenariokomponenten genutzt werden. In der Praxis ergibt sich daraus häufig ein hybrider Architekturansatz, in dem virtuelle Maschinen und Container je nach didaktischer und technischer Funktion kombiniert werden. Mit wachsender technischer Komplexität wird darüber hinaus eine Ebene der Orchestrierung erforderlich. Gerade in umfangreicheren Range-Umgebungen genügt es nicht, einzelne Container oder virtuelle Maschinen manuell zu starten und zu konfigurieren; vielmehr müssen Abhängigkeiten, Zustände, Skalierung, Netzwerkbeziehungen und Ausfallsicherheit automatisiert verwaltet werden. In containerisierten Umgebungen ist hierfür insbesondere Kubernetes relevant, das nach offizieller Beschreibung eine portable und erweiterbare Plattform zur Verwaltung containerisierter Workloads und Services bereitstellt und auf deklarative Konfiguration, Automatisierung und Skalierbarkeit ausgerichtet ist [73]. In Cyber-Ranges kann eine solche Orchestrierungsschicht dazu beitragen, Szenarien reproduzierbar bereitzustellen, unterschiedliche Team- oder Rollenbereiche voneinander zu trennen, Angriffs- und Verteidigungskomponenten dynamisch zuzuweisen und Ressourcen im Verlauf einer Übung bedarfsgerecht anzupassen. Aus curriculärer Perspektive ist dies deshalb wichtig, weil eine hohe Orchestrierbarkeit nicht nur den Betriebsaufwand reduziert, sondern auch die gezielte Variation von Szenarien, Komplexitätsstufen und Wiederholungen unterstützt.

Eine weitere tragende Komponente moderner Cyber Ranges ist die Automatisierung der Infrastruktur und Konfiguration. Hier kommen typischerweise Werkzeuge aus dem Bereich Infrastructure as Code und Configuration Management zum Einsatz. Terraform wird von HashiCorp als Infrastructure-as-Code-Tool beschrieben, mit dem Cloud- und On-Prem-Ressourcen in menschenlesbaren Konfigurationsdateien definiert, versioniert, wiederverwendet und über ihren gesamten Lebenszyklus verwaltet werden können [74]. Ansible ergänzt diese Ebene durch

agentenlose Automatisierung mit deklarativen, YAML-basierten Playbooks, die Konfiguration, Deployment und Orchestrierung über heterogene Infrastrukturen hinweg unterstützen [75]. Für Cyber Ranges bedeutet dies, dass nicht nur einzelne Systeme, sondern ganze Szenariowelten als Code beschrieben und automatisiert erzeugt werden können. Didaktisch ist dies besonders wertvoll, weil dadurch Trainingsumgebungen zwischen Übungsläufen konsistent zurückgesetzt, Varianten eines Szenarios vergleichbar ausgerollt und standardisierte Laborbedingungen für unterschiedliche Ausbildungsgruppen hergestellt werden können. Für Bumblebee ist diese Wiederholbarkeit ein wesentliches Qualitätsmerkmal, da nur so sichergestellt werden kann, dass Lernfortschritte, Fehlerbilder und Evaluierungsergebnisse nicht von zufälligen Umgebungsunterschieden verzerrt werden. Über die reine Bereitstellung technischer Systeme hinaus benötigen Cyber Ranges zusätzlich eine Schicht zur Szenario- und Verhaltenssimulation. Hierzu zählen insbesondere Werkzeuge, die Angreiferverhalten, Hintergrundrauschen, legitime Benutzeraktivität oder strukturierte Emulationskampagnen abbilden. Ein wichtiges Beispiel ist MITRE Caldera, das sich selbst als skalierbare Open-Source-Plattform für automatisierte Adversary Emulation, Sicherheitsbewertungen und Red-Team-Unterstützung beschreibt [76]. Caldera basiert auf dem MITRE ATT&CK-Framework und ermöglicht es, Angriffstechniken, Profile und Abläufe systematisch in Übungen einzuspeisen. Ergänzend dazu ist für realistische Hintergrundaktivität die Simulation legitimer Benutzerhandlungen bedeutsam. Hierfür ist etwa das von Carnegie Mellon SEI entwickelte GHOSTS Framework relevant, das als Open-Source-System zur Erzeugung komplexer NPC-Aktivität in Training, Übung und Simulation beschrieben wird und explizit für Cyber-Training, Cyber-Range-Entwicklung und realistische Netzwerkverhaltensmuster genutzt werden kann [77]. Für die didaktische Qualität einer Cyber Range ist diese Ebene zentral, weil realistische Angriffe und realistische Benutzeraktivität die Erkennungssituation erheblich komplexer und damit praxisnäher machen. Gerade im militärischen Kontext, in dem die Unterscheidung zwischen normalen, auffälligen und sicherheitsrelevanten Ereignissen eine Kernkompetenz darstellt, ist dies von besonderem Wert.

Neben Infrastruktur, Orchestrierung und Simulation benötigen Cyber Ranges außerdem Komponenten für Monitoring, Logging, Auswertung und Scoring. Diese Ebene ist nicht nur technisch erforderlich, um Systemzustände und Übungsabläufe sichtbar zu machen, sondern vor allem didaktisch und evaluativ bedeutsam. Nur wenn nachvollziehbar ist, welche Ereignisse aufgetreten sind, welche Entscheidungen getroffen wurden, welche Werkzeuge genutzt wurden und wie die Kommunikation innerhalb eines Szenarios verlaufen ist, lassen sich Leistungen der Teilnehmenden fundiert bewerten. In technisch einfacheren Umgebungen kann dies über klassische CTF-Mechanismen mit Punktevergabe und Flag-Submissions erfolgen; in anspruchsvolleren Cyber Ranges müssen darüber hinaus Prozessqualität, Reaktionszeit, Priorisierung, Dokumentation, Teamkoordination und Eskalationsverhalten berücksichtigt werden [70]. Daraus folgt, dass das Bewertungssystem eines Range-Stacks nicht auf technische Trefferlogik reduziert werden darf. Vielmehr sollte es so gestaltet sein, dass es sowohl technische Performanz als auch organisationsbezogene Handlungssicherheit erfasst. Für Bumblebee ist dies besonders relevant, da die Zielgruppe nicht primär offensive Wettbewerbsfähigkeiten entwickeln, sondern sicherheitsrelevante Ereignisse erkennen, einordnen, dokumentieren und regelgeleitet weiterverarbeiten soll.

Somit zeigt sich, dass der Technologie-Stack von Cyber Ranges aus mehreren komplementären Schichten besteht: einer skalierbaren Infrastrukturplattform, Virtualisierung und Containerisierung, Orchestrierungsmechanismen, Infrastructure-as-Code- und Automatisierungskomponenten, Szenario- und Verhaltenssimulation sowie Monitoring- und Auswertungssystemen [70][71][72][73][74][75][76][77]. Für das Projekt Bumblebee bedeutet dies, dass eine geeignete technische Architektur nicht monolithisch gedacht werden sollte, sondern als modularer Stack, dessen Komponenten gezielt entlang der didaktischen Anforderungen ausgewählt und kombiniert werden. Ein solcher Stack sollte insbesondere die kontrollierte Bereitstellung realistischer



Systemlandschaften, die Wiederverwendbarkeit von Szenarien, die Unterstützung rollenbasierter Übungen, die Nachvollziehbarkeit von Teilnehmerhandlungen und die Integration von Kommunikations- und Eskalationslogiken ermöglichen. Erst durch diese Kombination entsteht eine Trainingsumgebung, die nicht nur technisch funktionsfähig, sondern auch für die Entwicklung militärisch anschlussfähiger Cyberkompetenzen didaktisch tragfähig ist.

3.10 Auswahlkriterien für eine geeignete Trainingsplattform

Die Auswahl einer geeigneten Trainingsplattform oder Cyber Range ist keine primär technische Beschaffungsfrage, sondern eine didaktisch, organisatorisch und infrastrukturell zu begründende Systementscheidung. In der Forschung zu Cyber Ranges wird wiederholt darauf hingewiesen, dass Trainingsumgebungen nur dann wirksam sind, wenn ihre Architektur und ihre Funktionalitäten eng an den jeweiligen Lernzielen, Zielgruppen und Nutzungsszenarien ausgerichtet werden. Entsprechend sollte eine Plattform nicht nach dem Umfang ihrer Einzelfunktionen, sondern nach ihrer Eignung zur Unterstützung eines konkreten Ausbildungsauftrags bewertet werden. Für das Projekt Bumblebee bedeutet dies, dass die Plattformausswahl an den im Bedarfsprofil identifizierten Kernanforderungen – insbesondere Erkennung, Erstbewertung, Dokumentation, Kommunikation und Eskalation – auszurichten ist und nicht an einer möglichst allgemeinen oder maximal komplexen technischen Lösung. [70][80][81]

Ein erstes zentrales Auswahlkriterium ist die didaktische Passung zur Zielgruppe. Trainingsplattformen unterscheiden sich erheblich darin, ob sie für Einsteiger, fortgeschrittene Fachkräfte oder hochspezialisierte Teams ausgelegt sind. CISA beschreibt seine Cyber-Range-Trainings ausdrücklich als praxisnahe, instruktionsgeleitete Lab-Formate für Anfänger- und mittlere Erfahrungsstufen, während komplexere Range-Ansätze häufig deutlich höhere Eingangsvoraussetzungen implizieren. Für Bumblebee folgt daraus, dass die ausgewählte Umgebung einen gestuften Kompetenzaufbau unterstützen muss: Sie sollte sowohl niederschwellige Einstiege für Teilnehmende mit begrenztem Vorwissen ermöglichen als auch hinreichend realitätsnahe und technisch belastbare Szenarien für weiterführende Übungsphasen bereitstellen. Eine Plattform, die ausschließlich hochkomplexe Spezialtrainings unterstützt, wäre für ein grundlegendes operatives Ausbildungsprogramm ebenso ungeeignet wie eine Lösung, die nur elementare Aufgabenformate ohne Rollen-, Prozess- und Eskalationslogik anbietet. [55][70][77][80]

Ein zweites wesentliches Kriterium betrifft die Realitätsnähe beziehungsweise Fidelity der Trainingsumgebung. In der Fachliteratur wird Realismus als ein zentraler Wirksamkeitsfaktor von Cyber Ranges hervorgehoben, wobei nicht vollständige technische Perfektion, sondern eine für die jeweilige Lernaufgabe angemessene Abbildung realer System-, Netzwerk- und Bedrohungsbedingungen entscheidend ist. Der systematische Überblick zu Cyber-Range-Architekturen betont, dass sich Ranges unter anderem nach Simulations-, Emulations- und Hybridansätzen unterscheiden und dass diese Unterschiede unmittelbare Folgen für Skalierbarkeit, Kosten, Realitätsgrad und didaktischen Nutzen haben. Für Bumblebee ist daraus abzuleiten, dass die Plattform realistische, aber kontrollierbare Szenarien unterstützen sollte: ausreichend realitätsnah, um Log-Analyse, Monitoring, Incident Response und Kommunikationsprozesse glaubwürdig zu trainieren, jedoch zugleich so strukturiert, dass Wiederholung, Variation und didaktische Steuerung möglich bleiben. [59][60][61][80][81]

Das dritte Auswahlkriterium ist die Skalierbarkeit und Wiederholbarkeit der Umgebung. Trainingsplattformen und Cyber Ranges müssen in der Lage sein, Szenarien für unterschiedliche Gruppengrößen, Komplexitätsstufen und Wiederholungszyklen bereitzustellen. Gerade für Ausbildungsprogramme mit mehreren Durchläufen ist es entscheidend, dass Umgebungen standardisiert ausgerollt, nach Übungen in definierte Ausgangszustände zurückgesetzt und bei Bedarf angepasst werden können. Die Forschung zu Cyber-Range-Designs betont entsprechend die Bedeutung von Repeatability, Szenariokonfiguration und Lebenszyklusmanagement. Für Bumblebee ist dies besonders relevant, weil die Ausbildung nicht als einmalige Demonstration, sondern als wiederverwendbarer und evaluierbarer Ausbildungsprozess gedacht ist. Eine geeignete Plattform muss daher nicht nur technisch funktionieren, sondern Szenarien konsistent reproduzierbar und operativ beherrschbar machen. [70][74][75][80][81]

Ein viertes Kriterium betrifft die Isolation und Sicherheit der Trainingsumgebung. NIST beschreibt Cyber Ranges ausdrücklich als sichere beziehungsweise sandboxartige Umgebungen, in denen realitätsnahe Trainings und Challenges ohne Gefährdung produktiver Systeme durchgeführt werden können. Für militärische oder sicherheitskritische Kontexte ist diese Eigenschaft nicht nur technisch, sondern auch organisatorisch zentral. Die ausgewählte Plattform muss sicherstellen, dass Szenarien getrennt von operativen Netzen und realen Datenbeständen betrieben werden können, dass Angriffs- und Verteidigungswerkzeuge kontrolliert eingesetzt werden und dass keine ungewollten Seiteneffekte auf produktive Infrastrukturen entstehen. Daraus folgt für Bumblebee, dass On-Premise-Fähigkeit, Netzsegmentierung, kontrollierte Rechtevergabe und ein sauberer Umgang mit synthetischen oder simulierten Daten zu den zentralen Auswahlkriterien zählen sollten. [52][76][80]

Das fünfte Kriterium ist die Unterstützung rollen- und teambasierter Übungen. Für grundlegende technische Schulung können Einzellabore oder CTF-Formate ausreichend sein. Für ein militärisch orientiertes Ausbildungsprogramm genügt dies jedoch nicht, da dort auch Rollenverteilung, Meldekettens, kooperative Analyse, Eskalation und Kommunikation trainiert werden müssen. ENISA hebt bei Trainings und Exercises ausdrücklich hervor, dass solche Formate Kapazitätsaufbau, Gap-Identifikation und die koordinierte Reaktion auf komplexe Cyberlagen unterstützen. Auch groß angelegte Übungen wie NATO CCDCOE Locked Shields zeigen, dass der eigentliche Mehrwert anspruchsvoller Range-Umgebungen in der Verbindung technischer Verteidigung mit Kommunikation, Führung, Recht, Medienarbeit und organisationsbezogener Koordination liegt. Für Bumblebee bedeutet dies, dass eine Plattform bevorzugt werden sollte, die nicht nur Einzelaufgaben, sondern auch Teamrollen, Beobachter- oder White-Team-Funktionen, Kommunikationskanäle, Reporting und Debriefing unterstützt. [44][78][79]

Ein sechstes Auswahlkriterium betrifft die Beobachtbarkeit, Auswertbarkeit und Evaluationsfähigkeit der Umgebung. Cyber Ranges sind für Ausbildung nur dann nachhaltig nutzbar, wenn sich Teilnehmerhandlungen, Systemereignisse und Prozessverläufe nachvollziehbar erfassen lassen. Dazu gehören Logging, Monitoring, Zeitstempel, Ereigniskorrelation, Auswertung von Teilnehmerentscheidungen sowie – je nach Szenario – auch qualitative Beobachtung von Kommunikation und Rollenverhalten. CISA verweist in seinen Cyber-Range-Trainings auf Recovery-Debriefs, moderierte Diskussionen und fallbasierte Reflexion als integrale Bestandteile des Lernprozesses. Für Bumblebee ist dies zentral, weil die Plattform nicht nur zum Üben, sondern auch zur Bewertung von Lernfortschritten und zur Ableitung von Lessons Learned dienen soll. Entsprechend sollte die Auswahl nicht nur auf die Durchführung von Szenarien, sondern auch auf die Qualität von Debriefing, Scoring, Nachvollziehbarkeit und evidenzbasierter Leistungsbeurteilung achten. [70][77][80]

Das siebte Kriterium ist die Anpassbarkeit an organisationsspezifische und domänenspezifische Anforderungen. Die Forschung zu Cyber Ranges weist darauf hin, dass Übungsumgebungen je nach Zielsetzung unterschiedliche Infrastrukturen, Rollenprofile, Branchenlogiken und technische Spezifika abbilden müssen, etwa klassische IT, OT, Cloud, 5G oder hybride Umgebungen. Für Bumblebee ist insbesondere relevant, dass die Umgebung nicht nur generische Angriffs- und Verteidigungsszenarien unterstützt, sondern die Simulation organisationsbezogener Reaktionslogiken, typischer Monitoring- und Meldestrukturen sowie – perspektivisch – auch die Anbindung kritischer Infrastrukturaspekte ermöglicht. Damit wird Anpassbarkeit zu einem Kernkriterium: Eine Plattform sollte eigene Szenarien, Netzwerktopologien, Benutzerrollen, Aufgabenlogiken und Evaluationsmechanismen unterstützen, anstatt nur vorgefertigte Trainingsinhalte bereitzustellen. [61][69][80][83]

Schließlich ist auch die Betriebs- und Nachhaltigkeitsperspektive zu berücksichtigen. Eine technisch leistungsfähige Umgebung ist nur dann für ein langfristiges Ausbildungsprogramm geeignet, wenn sie mit vertretbarem Aufwand betrieben, erweitert, gepflegt und weiterentwickelt



werden kann. Dazu zählen Fragen der Lizenzierung, der Abhängigkeit von proprietären Komponenten, der Automatisierbarkeit des Betriebs, der Verfügbarkeit von Dokumentation sowie der Möglichkeit, Inhalte und Infrastruktur über längere Zeiträume stabil weiterzuführen. Für Bumblebee spricht dies eher für einen modularen, möglichst offenen Technologieansatz, bei dem einzelne Komponenten austauschbar bleiben und die Plattform schrittweise ausgebaut werden kann. Gerade im militärischen Umfeld ist Nachhaltigkeit auch deshalb entscheidend, weil Ausbildungsumgebungen nicht nur kurzfristig innovativ, sondern mittelfristig verlässlich, kontrollierbar und institutionell anschlussfähig sein müssen. [69][71][74][75][80][81]

3.11 Implikationen für das Projekt Bumblebee

Aus der vorangegangenen Analyse von Lernplattformen, Cyber-Ranges, Technologie-Stacks und Auswahlkriterien ergibt sich für das Projekt Bumblebee, dass eine isolierte Orientierung an klassischen Lernplattformen oder CTF-Formaten für die angestrebten Ausbildungsziele nicht ausreicht. Solche Plattformen sind zwar geeignet, technische Grundlagen, Tool-Kompetenzen und erste analytische Fähigkeiten aufzubauen, sie bilden jedoch organisationsbezogene Abläufe, Meldekettens, Kommunikationsprozesse und rollenbasierte Reaktionslogiken nur eingeschränkt ab. Für Bumblebee, dessen Zielgruppe auf operative Erstreaktions- und Unterstützungsfunktionen im SOC-/NOC-nahen Kontext vorbereitet werden soll, ist daher ein Ausbildungssystem erforderlich, das technische Übung mit organisatorischer Handlungsfähigkeit systematisch verbindet. Diese Schlussfolgerung wird auch durch europäische und internationale Trainingsansätze gestützt: ENISA betont den Wert von Trainings und Exercises für Capacity Building, Gap-Identifikation und koordinierte Reaktion, CISA setzt bei Incident-Response-Trainings auf realistische, instruktionsgeleitete Cyber-Range-Labs, und Locked Shields zeigt exemplarisch, dass wirksame Cyberausbildung technische Verteidigung, strategische Entscheidungen, Kommunikation, Recht und Führung zusammenführen muss.

Für Bumblebee spricht dies für einen mehrschichtigen Ausbildungsansatz, in dem unterschiedliche Plattfortmtypen jeweils klar definierte Funktionen übernehmen. Ein erstes Ausbildungsniveau sollte auf den Aufbau grundlegender technischer Kompetenzen ausgerichtet sein, etwa in den Bereichen Netzwerke, Linux, Logging, Monitoring, SIEM-Verständnis und Basisformen der Incident Detection. Hierfür können stärker didaktisch geführte Trainingsplattformen sinnvoll eingesetzt werden. Aufbauend darauf sollte jedoch eine zweite Ebene eingeführt werden, in der realitätsnahe und rollenbezogene Szenarien trainiert werden. Diese Ebene muss in der Lage sein, sicherheitsrelevante Ereignisse nicht nur technisch sichtbar zu machen, sondern auch Dokumentation, Priorisierung, Lagebildarstellung, interne Kommunikation und die regelgeleitete Weiterleitung an zuständige Stellen abzubilden. Gerade diese Verbindung von Technik und Prozesslogik erscheint als zentrale curriculare Konsequenz aus der Bedarfsanalyse und wird zugleich durch internationale Übungsmodelle bestätigt, die Incident Response ausdrücklich als technischen und organisatorischen Gesamtprozess behandeln. Ein weiterer wesentlicher Befund betrifft die didaktische Progression. Für Bumblebee erscheint es weder zielführend, unmittelbar mit hochkomplexen „live-fire“-Szenarien zu beginnen, noch die Ausbildung dauerhaft auf niedrigschwellige Einzelaufgaben zu begrenzen. Vielmehr spricht die Analyse für ein gestuftes Modell, in dem Teilnehmende zunächst in kontrollierten und angeleiteten Umgebungen grundlegende operationale Routinen aufbauen und diese anschließend in komplexeren, stärker dynamischen Team- und Eskalationsszenarien anwenden. CISA beschreibt seine Range-Trainings entsprechend als guided step-action labs für Beginner- und Intermediate-Analysten, während ENISA bei Cyber Europe die Fähigkeit betont, komplexe technische Vorfälle, Krisenmanagement und organisationsübergreifende Koordination unter realistischen Bedingungen zu trainieren. Daraus lässt sich für Bumblebee ableiten, dass die Trainingsumgebung sowohl Einsteigerpfade als auch fortgeschrittene Szenariostufen unterstützen muss, damit heterogene Zielgruppen mit unterschiedlichem Vorwissen auf einem gemeinsamen Kompetenzpfad entwickelt werden können.

Für die technische Umsetzung ergibt sich daraus, dass Bumblebee nicht auf eine einzelne monolithische Plattformtechnologie festgelegt werden sollte. Zielführender erscheint ein modulares Trainingsökosystem, das Lernplattformen, Lab-Umgebungen und Range-Komponenten kombiniert. Eine solche Architektur sollte insbesondere die isolierte Bereitstellung realistischer Netzwerk- und Systemlandschaften, die Wiederholbarkeit von Szenarien, die flexible Zuweisung von Rollen und die technische Beobachtbarkeit von Übungen ermöglichen. Ebenso wichtig ist die Fähigkeit, Szenarien entlang didaktischer Ziele schrittweise zu erweitern – etwa von der Einzelanalyse eines verdächtigen Ereignisses bis hin zur koordinierten Bearbeitung eines

komplexen, organisationsübergreifenden Vorfalles. Damit folgt für Bumblebee aus den untersuchten Best Practices, dass nicht die maximal mögliche technische Komplexität den Ausschlag geben sollte, sondern die didaktisch kontrollierte Übersetzbarkeit realer Cyberlagen in trainierbare Lern- und Handlungssituationen. Dies entspricht auch dem Ansatz der AIT Cyber Range, die praktische IT- und OT-Use-Cases, Skill Development über unterschiedliche Zielgruppen hinweg sowie nationale Übungsformate für kritische Infrastrukturen miteinander verbindet. Darüber hinaus legt die Analyse nahe, dass Bumblebee die Team- und Führungsdimension von Cybervorfällen ausdrücklich berücksichtigen sollte. Internationale Übungsmodelle wie Locked Shields zeigen, dass die eigentliche Herausforderung anspruchsvoller Cyberlagen nicht nur in der technischen Abwehr besteht, sondern in der Verbindung von technischer Analyse, Berichtswesen, Entscheidungsunterstützung, Rechts- und Kommunikationsfragen sowie der Zusammenarbeit entlang der chain of command. Auch ENISA betont bei Cyber Europe den Mehrwert realistischer, großskaliger Krisenszenarien für die Entwicklung technischer, operativer und strategischer Fähigkeiten. Für Bumblebee bedeutet dies, dass Trainingsumgebungen nicht ausschließlich auf individuelle Tool-Nutzung oder Challenge-Lösungen ausgerichtet sein sollten. Vielmehr sollten auch Rollen wie Analyst, First Responder, Team Lead, Meldeverantwortliche oder Beobachter/White Team explizit in die Szenarien integriert werden, um organisationsbezogene Handlungssicherheit aufzubauen.

Schließlich hat die Analyse auch Implikationen für die strategische Positionierung von Bumblebee als Ausbildungsprogramm. Ein tragfähiges militärisches Cybertraining sollte nicht versuchen, existierende internationale Spitzenmodelle vollständig zu replizieren. Weder großskalige multinational ausgerichtete Übungen wie Locked Shields noch breit ausdifferenzierte nationale Trainingsökosysteme lassen sich ohne Weiteres auf kleinere, zielgruppenspezifische Ausbildungsprogramme übertragen. Der Mehrwert solcher Modelle liegt vielmehr darin, zentrale Strukturprinzipien sichtbar zu machen: Realitätsnähe, Rollenbezug, Wiederholbarkeit, kontrollierte Eskalation, Debriefing-Fähigkeit und die Verbindung von technischer und organisatorischer Reaktion. Für Bumblebee folgt daraus, dass ein eigenständiger, modularer und schrittweise ausbaubarer Ansatz am sinnvollsten erscheint, der auf grundlegende operative Kompetenzentwicklung zielt und zugleich offen bleibt für spätere Erweiterungen in Richtung komplexerer Team- und Krisenszenarien. In dieser Perspektive sollte die Trainingsumgebung von Bumblebee nicht nur als technische Plattform verstanden werden, sondern als didaktisch strukturierter Handlungsraum, in dem technische Basiskompetenz, standardisierte Melde- und Reaktionsprozesse sowie militärisch anschlussfähige Koordinationsfähigkeit gemeinsam eingeübt werden können.

3.12 Parameter und Indikatoren für die Aus- und Fortbildung im militärischen SOC-/NOC-Kontext

Auf Grundlage der vorangegangenen Analysen werden im Folgenden Parameter und Indikatoren definiert, mit denen die Zielerreichung des geplanten Aus- und Fortbildungsprogramms systematisch bewertet werden kann. Die Indikatoren dienen nicht der Bewertung realer militärischer Operationen, sondern der Evaluierung von Ausbildungsqualität, Kompetenzaufbau und Übungsleistung in kontrollierten Trainingskontexten.

Ziel ist es, die Wirksamkeit des Curriculums nicht nur inhaltlich zu begründen, sondern über nachvollziehbare Kriterien empirisch überprüfbar zu machen. Die Ableitung erfolgt entlang dreier komplementärer Dimensionen: technischer Kompetenzvermittlung, organisatorischer Handlungsfähigkeit und individueller Trainingsbedürfnisse.

TABELLE 1 PARAMETER UND INDIKATOREN MATRIX

Kategorie	Indikator	Messmethode	Zielbezug	Datenquelle
Technische Vermittlung	Erkennungsfähigkeit sicherheitsrelevanter Ereignisse	Szenariobasierte Übung, Vorher-Nachher-Vergleich	Frühzeitige Identifikation und Erstbewertung	Praxistest, Beobachtungsbogen
Technische Vermittlung	Handlungssicherheit bei SIEM- und Logdaten	Aufgabenbearbeitung mit Logquellen und SIEM	Korrekte Einordnung relevanter Ereignisse	Auswertung der Übungsartefakte
Organisatorisches Design	Anwendung der Melde- und Eskalationskette	Rollenspiel, Lage- und Eskalationsszenario	Regelkonforme Weiterleitung	Trainerbeobachtung, Dokumentationsprüfung
Organisatorisches Design	Vollständigkeit der Vorfalldokumentation	Checkliste, Dokumentenreview	Nachvollziehbare Lagebilderstellung	Meldeformular, Incident-Log
Individuelle Trainingsbedürfnisse	Lernfortschritt und Passung des Ausbildungsniveaus	Eingangserhebung, Abschlussbewertung, Feedback	Kompetenzzuwachs trotz heterogener Vorkenntnisse	Tests, Feedbackbogen

Die Tabelle fasst zentrale Evaluierungsbereiche in verdichteter Form zusammen und dient als operative Brücke zwischen konzeptioneller Anforderungsanalyse und späterer Umsetzung in Lernzielkontrollen, Übungsauswertung und Qualitätsmanagement.

3.12.1 Cybersecurity-relevante technische Vermittlung

In dieser Kategorie wird untersucht, inwieweit das Ausbildungsprogramm jene technischen Grundkompetenzen vermittelt, die für den Einsatz im militärischen SOC- und NOC-Umfeld erforderlich sind. Im Zentrum steht dabei kein spezialisiertes Expertenwissen, wie es etwa in der digitalen Forensik, der Malware-Entwicklung oder der sicherheitsbezogenen Softwareentwicklung erforderlich wäre, sondern ein anwendungsorientiertes Kompetenzprofil auf operativer Ebene. Ziel ist es, Teilnehmende zu befähigen, sicherheitsrelevante Auffälligkeiten in IT- und Kommunikationssystemen frühzeitig zu erkennen, diese in ihrem situativen Kontext einzuordnen, erste strukturierte Analysen durchzuführen und auf dieser Grundlage angemessene Erstmaßnahmen im Sinne definierter Prozesse einzuleiten. Diese Schwerpunktsetzung entspricht dem im Deliverable beschriebenen Ausbildungsziel, wonach die Zielgruppe vor allem bestehende Systeme überwachen, Auffälligkeiten bewerten und Vorfälle regelgeleitet an zuständige Stellen weiterleiten soll.

Die technische Vermittlung ist dabei nicht isoliert zu betrachten, sondern als Bestandteil einer handlungsorientierten Kompetenzentwicklung. Für den militärischen Ausbildungszusammenhang

ist von besonderer Bedeutung, dass technische Beobachtungen nicht lediglich reproduziert, sondern in eine belastbare Lageeinschätzung überführt werden können. Dies setzt voraus, dass die Teilnehmenden grundlegende Kenntnisse über System- und Netzwerkinfrastrukturen, typische Angriffsmuster, sicherheitsrelevante Indikatoren, Logquellen sowie standardisierte Incident-Response-Abläufe erwerben. Das Deliverable zeigt hierzu einen klaren Bedarf in den Bereichen SIEM, Loganalyse, Netzwerkgrundlagen und strukturierte Vorfallsbehandlung; zugleich wird betont, dass zukünftige Ausbildungsformate praxisnah, gestuft und an realistischen Bedrohungsszenarien orientiert sein sollen.

Ein zentraler Indikator innerhalb dieser Kategorie ist die Erkennungsfähigkeit sicherheitsrelevanter Ereignisse. Diese beschreibt die Fähigkeit der Teilnehmenden, zwischen regulären Betriebsereignissen und potenziell sicherheitskritischen Auffälligkeiten zu unterscheiden. Aus didaktischer und evaluativer Perspektive ist diese Fähigkeit von hoher Relevanz, da sie die Grundlage jeder weiteren Incident-Bearbeitung bildet. Im Rahmen einer Abschlussübung gilt dieser Indikator als erreicht, wenn die Teilnehmenden einen überwiegenden Anteil der vorbereiteten sicherheitsrelevanten Ereignisse korrekt identifizieren und zutreffend klassifizieren. Die Messung kann über szenariobasierte Aufgaben mit definierten Erwartungshorizonten erfolgen. Als Zielwert kann festgelegt werden, dass mindestens 80 % der Teilnehmenden mindestens 75 % der vorgegebenen Ereignisse korrekt als sicherheitsrelevant oder nicht sicherheitsrelevant einordnen. Damit wird nicht nur reines Faktenwissen überprüft, sondern die Fähigkeit zur situativen Differenzierung unter realitätsnahen Bedingungen. Ein weiterer wesentlicher Indikator ist die Qualität der Erstanalyse. Diese bezieht sich auf die Fähigkeit, einen erkannten Vorfall in strukturierter Form zu beschreiben und erste Hypothesen zur Art, Tragweite und Dringlichkeit des Ereignisses abzuleiten. Eine fachlich belastbare Erstanalyse umfasst zumindest die Benennung betroffener Systeme oder Dienste, die Beschreibung beobachteter Symptome, die vorläufige Einordnung der vermuteten Ereignisart sowie die Ableitung erster empfohlener Schritte. Im militärischen Kontext ist diese Kompetenz besonders relevant, da zwischen der initialen Beobachtung vor Ort und der weiterführenden Bearbeitung durch spezialisierte Stellen häufig eine Übergabeschnittstelle besteht. Die Qualität der Erstanalyse bestimmt somit wesentlich die Anschlussfähigkeit nachfolgender Reaktions- und Eskalationsprozesse. Als erfüllt kann der Indikator gelten, wenn mindestens 75 % der Teilnehmenden in einer standardisierten Abschlussübung eine fachlich nachvollziehbare und hinreichend vollständige Erstanalyse ohne kritische Auslassungen dokumentieren.

Ergänzend ist die Handlungssicherheit im Umgang mit SIEM- und Logdaten als eigenständiger Indikator zu betrachten. Diese umfasst die Fähigkeit, relevante Logeinträge, Alarme, Korrelationen und Anomalien zu erfassen, ihre Bedeutung für die Sicherheitslage einzuschätzen und daraus eine begründete erste Bewertung abzuleiten. Das Deliverable weist ausdrücklich darauf hin, dass in der Zielgruppe bislang nur geringe Vorerfahrungen mit SIEM-Systemen vorhanden waren und deshalb ein curricularer Bedarf für einführende Module in SIEM-Technologien und Linux-Grundlagen besteht. Vor diesem Hintergrund ist die sichere Nutzung von SIEM- und Logdaten nicht nur ein Lernziel, sondern zugleich ein Gradmesser dafür, ob das Ausbildungsdesign die notwendige didaktische Progression erfolgreich umgesetzt hat. Der Indikator ist erreicht, wenn mindestens 70 % der Teilnehmenden in einer Loganalyse-Aufgabe die wesentlichen Artefakte korrekt identifizieren und eine sachlich plausible Einschätzung des Ereignisses formulieren. Für den konkreten SOC-/NOC-Bezug ist darüber hinaus die Anwendung technischer Erstmaßnahmen von hoher Relevanz. Diese beschreibt die Fähigkeit, auf Basis einer ersten Lageeinschätzung solche Maßnahmen auszuwählen, die im Rahmen der eigenen Rolle zulässig, zweckmäßig und prozesskonform sind. Dazu zählen etwa das Isolieren betroffener Systeme, die strukturierte Meldung an zuständige Stellen, die Sicherung relevanter Informationen, die Erstellung eines ersten Lagebildes oder die abgestimmte Übergabe an eine übergeordnete Incident-Response-Funktion. Im militärischen Umfeld ist diese Kompetenz besonders sensibel, da Erstmaßnahmen nicht nur

technisch angemessen, sondern auch in Kommunikations- und Eskalationsstrukturen eingebettet sein müssen. Entsprechend ist nicht allein entscheidend, ob überhaupt gehandelt wird, sondern ob dies in regelkonformer, lageangepasster und nicht eskalationsverschärfender Weise erfolgt. Als erfüllt gilt der Indikator, wenn mindestens 80 % der Teilnehmenden in einem Übungsszenario keine fachlich kontraindizierten Sofortmaßnahmen setzen und ihre Handlungsauswahl plausibel begründen können.

3.12.2 Organisatorisches Design

Diese Kategorie erfasst, inwieweit das Ausbildungsprogramm nicht nur technisches Fachwissen vermittelt, sondern zugleich jene organisatorischen Strukturen, Prozesse und Handlungslogiken abbildet, die für den militärischen Einsatzkontext von zentraler Bedeutung sind. Im Unterschied zu rein technisch orientierten Ausbildungsansätzen wird dabei davon ausgegangen, dass die Wirksamkeit von Cybersicherheitskompetenz wesentlich davon abhängt, ob diese in bestehende Melde-, Kommunikations- und Eskalationsstrukturen eingebettet werden kann. Gerade im militärischen Umfeld erfolgen die Behandlung von Sicherheitsvorfällen, die Priorisierung von Maßnahmen sowie die operative Entscheidungsfindung nicht isoliert auf individueller Ebene, sondern im Rahmen formalisierter Zuständigkeiten, hierarchischer Kommunikationswege und definierter Reaktionsprozesse. Die organisatorische Einbettung stellt daher keinen ergänzenden Aspekt, sondern einen konstitutiven Bestandteil professioneller Handlungsfähigkeit im SOC- und NOC-Kontext dar.

Für die Zielgruppe des geplanten Ausbildungsprogramms ist dies besonders relevant, da sie nach den Ergebnissen der Bedarfserhebung primär nicht auf hochspezialisierte Analyse- oder Forensikaufgaben vorbereitet werden soll, sondern auf die frühzeitige Erkennung von Vorfällen, deren strukturierte Weiterleitung sowie die Einleitung regelkonformer Erstreaktionen. Daraus folgt, dass organisatorische Kompetenzen – etwa im Bereich Meldewege, Rollenverständnis, Berichtswesen und Eskalationslogik – im Curriculum denselben Stellenwert erhalten müssen wie technische Basiskompetenzen. Ausbildungsqualität ist in dieser Kategorie folglich daran zu messen, ob die Teilnehmenden lernen, sicherheitsrelevante Ereignisse nicht nur technisch zu bewerten, sondern diese auch innerhalb der vorgesehenen Organisationsstrukturen korrekt zu verorten und weiterzuverarbeiten.

Ein erster zentraler Indikator ist die korrekte Anwendung der Melde- und Eskalationskette. Dieser Indikator beschreibt die Fähigkeit der Teilnehmenden, einen erkannten Vorfall an die zuständige Stelle, zum angemessenen Zeitpunkt und über den vorgesehenen Kommunikationsweg weiterzugeben. Im militärischen Kontext besitzt diese Kompetenz besondere Relevanz, da Verzögerungen, Fehladressierungen oder informelle Kommunikationswege die Wirksamkeit der Incident Response erheblich beeinträchtigen können. Das Deliverable betont in diesem Zusammenhang ausdrücklich die Bedeutung klar definierter Kommunikationsstrukturen, etwa zwischen Personal vor Ort, First Respondern und zentralen Fachstellen, sowie die Notwendigkeit, auch alternative Kommunikationswege für eingeschränkte oder gestörte Infrastrukturen vorzusehen. Die Anwendung der Eskalationskette ist daher nicht lediglich als administrativer Vorgang zu verstehen, sondern als Teil der operativen Reaktionsfähigkeit. Der Indikator kann als erfüllt gelten, wenn mindestens 80 % der Teilnehmenden in einem szenariobasierten Übungssetting die vorgegebene Melde- und Eskalationskette vollständig korrekt anwenden.

Ein weiterer wesentlicher Indikator ist die Vollständigkeit der Vorfalldokumentation. Diese umfasst die Fähigkeit, sicherheitsrelevante Ereignisse in einer Weise zu erfassen, die für nachgelagerte Bearbeitungsschritte, Lagebilderstellung und organisationsübergreifende Übergaben anschlussfähig ist. Aus wissenschaftlich-didaktischer Perspektive erfüllt Dokumentation dabei mehrere Funktionen zugleich: Sie dient der formalen Nachvollziehbarkeit von Ereignissen, der Standardisierung von Informationsweitergabe, der Qualitätssicherung in Reaktionsprozessen

sowie der späteren Auswertung im Sinne von Debriefing und Lessons Learned. Im Deliverable wird wiederholt hervorgehoben, dass die strukturierte Incident-Dokumentation zu den Kernzielen der Ausbildung zählt und dass Teilnehmende in der Lage sein sollen, relevante Ereignisse geordnet an zuständige Fachstellen zu übermitteln. Als Mindestanforderung sollten Incident Reports daher Angaben zu Zeitpunkt, betroffenen Systemen, beobachteten Symptomen, gesetzten Erstmaßnahmen, Dringlichkeitseinschätzung und Weiterleitung enthalten. Der Indikator gilt als erfüllt, wenn mindestens 75 % der erstellten Berichte alle verpflichtend definierten Dokumentationselemente vollständig und nachvollziehbar enthalten.

Zusätzlich ist die Qualität des organisatorischen Übungsdesigns als eigenständiger Evaluierungsindikator zu berücksichtigen. Dieser bezieht sich nicht primär auf die Leistung einzelner Teilnehmender, sondern auf die Frage, ob die Ausbildungsumgebung selbst geeignet ist, organisationsbezogene Handlungskompetenzen realitätsnah zu fördern. Das Deliverable zeigt deutlich, dass für militärische Ausbildungsziele reine Einzelaufgaben oder rein technische Challenge-Formate nicht ausreichen, sondern durch Übungen ergänzt werden müssen, die Rollenverteilung, Kommunikationsanforderungen, Entscheidungsdruck, Lagebildarbeit, Teamkoordination und abgestufte Eskalation abbilden. Cyber Ranges und vergleichbare Trainingsumgebungen werden gerade deshalb als besonders geeignet beschrieben, weil sie neben technischen Reaktionen auch Kommunikation, Koordination und Zusammenarbeit zwischen lokalen Kräften und zentralen Stellen trainierbar machen. Die Qualität des organisatorischen Übungsdesigns ist demnach dann gegeben, wenn Kernübungen nicht nur technische Aufgabenstellungen, sondern auch kommunikative und organisatorische Bewertungselemente systematisch integrieren. Als erfüllt kann dieser Indikator gelten, wenn alle vorgesehenen Kernübungen mindestens ein technisches, ein kommunikatives und ein organisatorisches Bewertungselement enthalten.

Für das Ausbildungsprogramm der Trainerinnen und Trainer ist in dieser Kategorie zudem die didaktisch konsistente Durchführung von hoher Bedeutung. Organisatorische Handlungskompetenz kann nur dann verlässlich vermittelt und bewertet werden, wenn Briefing, Übungsbegleitung, Beobachtung und Debriefing nach einheitlichen didaktischen Grundsätzen erfolgen. Im Deliverable wird hervorgehoben, dass die Zielgruppe praxisnahe Lern- und Prüfungsformate bevorzugt, zugleich aber eine stärkere theoretische Vorbereitung, ein strukturierteres Onboarding und konstruktives Feedback einfordert. Ebenso wird darauf verwiesen, dass Lehrpersonal im militärischen Kontext verpflichtende pädagogische und didaktische Ausbildungen absolvieren muss. Daraus ergibt sich, dass die Qualität der Ausbildung nicht allein von der Fachkompetenz der Trainerinnen und Trainer abhängt, sondern auch von der Standardisierung didaktischer Abläufe und der konsistenten Anwendung gemeinsamer Bewertungsmaßstäbe. Der entsprechende Indikator ist erreicht, wenn alle eingesetzten Trainerinnen und Trainer auf Basis eines einheitlichen Leitfadens Briefing, Übungsbegleitung und Debriefing durchführen und dies nachvollziehbar dokumentieren. Als Zielwert kann festgelegt werden, dass 100 % der eingesetzten Trainerinnen und Trainer den standardisierten Ablauf verwenden.

3.12.3 Individuelle Trainingsbedürfnisse

Da die Zielgruppe hinsichtlich Vorwissen, technischer Erfahrung und Bildungsbiografie heterogen zusammengesetzt ist, muss das Ausbildungsprogramm unterschiedliche Ausgangsniveaus systematisch berücksichtigen. Im Zentrum dieser Kategorie steht daher die Frage, inwieweit das Ausbildungsdesign geeignet ist, sowohl Einsteigerinnen und Einsteiger als auch Teilnehmende mit Vorerfahrung angemessen zu adressieren, ohne dabei entweder Unterforderung oder Überforderung zu erzeugen. Für die Bewertung der Ausbildungsqualität ist dies von besonderer Relevanz, da Lernerfolg im Bereich der Cybersicherheitsausbildung nicht allein von der Qualität

der Inhalte abhängt, sondern in hohem Maß auch von deren didaktischer Passung zur Zielgruppe. Das Deliverable zeigt deutlich, dass innerhalb der untersuchten Kohorte erhebliche Unterschiede sowohl im Bereich der Vorkenntnisse als auch im formalen Bildungsniveau bestanden. Zugleich wurde bereits in der frühen Bedarfserhebung betont, dass kein verpflichtendes Vorwissen vorausgesetzt werden sollte, um unterschiedliche technische Hintergründe in die Ausbildung einbeziehen zu können. Daraus folgt, dass ein wirksames Curriculum im militärischen SOC-/NOC-Kontext eine adaptive oder zumindest gestufte Struktur aufweisen muss, die einen gemeinsamen Kompetenzaufbau ermöglicht, ohne die Heterogenität der Lernvoraussetzungen zu ignorieren. Diese Kategorie ist deshalb nicht nur als ergänzende didaktische Perspektive zu verstehen, sondern als eigenständiger Erfolgsfaktor des Ausbildungsprogramms. Während die technischen und organisatorischen Kategorien primär auf die Vermittlung spezifischer Fach- und Prozesskompetenzen abzielen, untersucht dieser Bereich, ob die Ausbildung in ihrer methodischen Anlage überhaupt geeignet ist, die Zielgruppe in ihrer Breite zu erreichen. Im militärischen Ausbildungskontext ist dies besonders bedeutsam, da Ausbildung häufig unter begrenzten Zeitressourcen erfolgt und gleichzeitig auf eine verlässliche Mindestqualifikation für operative Rollen hinwirken muss. Ein Ausbildungsdesign, das die unterschiedlichen Lernvoraussetzungen nicht berücksichtigt, läuft Gefahr, einerseits Vorkenntnisarme zu verlieren und andererseits Fortgeschrittene didaktisch nicht hinreichend zu fordern. Die Berücksichtigung individueller Trainingsbedürfnisse ist daher als Voraussetzung dafür zu verstehen, dass die übrigen Ausbildungsziele überhaupt wirksam umgesetzt werden können.

Ein wesentlicher Indikator in dieser Kategorie ist die Lernfortschrittsmessung zwischen Eingangserhebung und Abschlussbewertung. Dieser Indikator beschreibt, ob Teilnehmende im Verlauf der Ausbildung einen messbaren Kompetenzzuwachs erreichen, unabhängig von ihrem jeweiligen Ausgangsniveau. Aus evaluativer Sicht ist dies besonders relevant, da nicht allein das absolute Endniveau, sondern auch die Entwicklung über den Ausbildungszeitraum hinweg Aufschluss über die Wirksamkeit des Curriculums gibt. Im Deliverable wurde vorgeschlagen, zu Beginn bestimmter Module eine kurze Überprüfung vorhandener Kenntnisse durchzuführen; zugleich zeigen die Workshop-Ergebnisse, dass in mehreren inhaltlichen Bereichen – etwa bei SIEM, Linux sowie ausgewählten Standards und Frameworks – deutliche Ausgangsunterschiede bestanden. Eine systematische Lernfortschrittsmessung erlaubt es daher, den Kompetenzzuwachs differenziert zu erfassen und die Wirksamkeit einzelner Module zu bewerten. Der Indikator kann als erfüllt gelten, wenn mindestens 80 % der Teilnehmenden ihren Ergebniswert zwischen Vorabtest und Abschlusstest um mindestens 20 % steigern. Damit wird nicht nur die Wissensvermittlung überprüft, sondern auch die Frage, ob die Ausbildung für unterschiedliche Ausgangsniveaus lernwirksam gestaltet wurde.

Ein weiterer zentraler Indikator ist die Passung des Ausbildungsniveaus zur Zielgruppe. Diese beschreibt, ob die Schwierigkeit, das Lerntempo und die methodische Aufbereitung der Inhalte von der Mehrheit der Teilnehmenden als angemessen wahrgenommen werden. Eine hohe Passung ist insbesondere in heterogenen Lerngruppen wesentlich, da didaktische Fehlanpassungen unmittelbare Auswirkungen auf Motivation, Selbstwirksamkeit und Lernerfolg haben können. Im Rahmen der Bedarfserhebung wurde sichtbar, dass bestimmte praktische Einheiten – etwa im Umgang mit SIEM-Systemen – von allen Teilnehmenden als hoch oder sehr hoch schwierig eingeschätzt wurden, was auf fehlende vorbereitende Grundlagen hinweist. Gleichzeitig bestand ein ausgeprägter Wunsch nach stärkerer theoretischer Vorbereitung und nach einem strukturierteren Onboarding vor praktischen Übungen. Diese Befunde machen deutlich, dass die Schwierigkeit einer Ausbildung nicht allein inhaltlich, sondern immer auch in Relation zum Ausgangsniveau der Zielgruppe zu bewerten ist. Der Indikator ist erfüllt, wenn mindestens 75 % der Teilnehmenden die Schwierigkeitsstufe in der Abschlussevaluierung als angemessen oder überwiegend angemessen einstufen. Ergänzend wird die wahrgenommene Relevanz der Inhalte für die spätere Rolle im militärischen SOC-/NOC-Umfeld erhoben. Dieser Indikator zielt darauf ab,

ob die vermittelten Inhalte von den Teilnehmenden nicht nur verstanden, sondern auch als funktional und einsatznah bewertet werden. Aus didaktischer Perspektive ist die subjektive Relevanzwahrnehmung ein wichtiger Faktor für Lernmotivation, Engagement und Transferbereitschaft. Das Deliverable zeigt, dass die Zielgruppe praxisnahe Inhalte mit Bezug zu realistischen Angriffsszenarien als besonders motivierend und bedeutsam wahrnahm. Gleichzeitig wurden Themeninteressen benannt, die klare Hinweise auf die spätere Rollenorientierung geben, etwa in den Bereichen System- und Netzwerksicherheit, SIEM und Threat Hunting. Daraus folgt, dass Ausbildungsinhalte dann als besonders wirksam gelten können, wenn sie nicht als abstrakte Theorie, sondern als nachvollziehbare Vorbereitung auf konkrete Aufgaben im militärischen Cyberkontext erlebt werden. Der Indikator ist erreicht, wenn mindestens 80 % der Teilnehmenden die Relevanz der Ausbildungsinhalte für ihre spätere Funktion als hoch oder sehr hoch bewerten.

Für Trainerinnen und Trainer ist in dieser Kategorie außerdem die Qualität des Feedbacks und der Lernbegleitung von zentraler Bedeutung. Gerade in heterogenen Gruppen reicht es nicht aus, Inhalte lediglich bereitzustellen; vielmehr bedarf es einer lernprozessbegleitenden Unterstützung, die individuelle Verständnisschwierigkeiten aufgreift, Fortschritte sichtbar macht und Orientierung im Lernprozess bietet. Im qualitativen Feedback des Workshops wurde deutlich, dass von Trainerinnen und Trainern neben Fachkompetenz und Praxiserfahrung insbesondere Geduld und die Fähigkeit zu konstruktivem Feedback erwartet werden. Diese Rückmeldung verweist darauf, dass Lernbegleitung im vorliegenden Kontext nicht nur als sozialer Zusatzaspekt, sondern als didaktische Kernfunktion zu betrachten ist. Besonders in praxisorientierten Cyber-Übungen, in denen Unsicherheiten, Zeitdruck und technisches Neuland zusammenkommen, kann qualitativ hochwertiges Feedback entscheidend dafür sein, ob Lernende Fehler produktiv verarbeiten und in Handlungswissen überführen können. Der entsprechende Indikator ist erfüllt, wenn mindestens 80 % der Teilnehmenden das erhaltene Feedback als fachlich hilfreich, verständlich und unterstützend bewerten. Über diese einzelnen Indikatoren hinaus verweist die Kategorie auf die Notwendigkeit eines didaktisch gestuften Ausbildungskonzepts. Die im Deliverable dokumentierten Erkenntnisse legen nahe, dass insbesondere vor praktischen Übungen vorbereitende Theorieeinheiten, Tool-Einführungen und diagnostische Einstiegselemente erforderlich sind, um eine belastbare gemeinsame Ausgangsbasis zu schaffen. Heterogenität sollte daher nicht als Defizit der Zielgruppe verstanden werden, sondern als Planungsprämisse des Curriculums. Ein wissenschaftlich fundiertes Ausbildungsdesign im militärischen SOC-/NOC-Kontext muss folglich sowohl Differenzierung als auch Anschlussfähigkeit gewährleisten: Einsteigerinnen und Einsteiger benötigen klare Struktur, Einführung und schrittweise Progression, während Teilnehmende mit Vorerfahrung durch anspruchsvollere Anwendungsszenarien, vertiefende Übungen und erweiterte Reflexionsaufgaben eingebunden werden sollten. Die Qualität der Ausbildung bemisst sich in dieser Kategorie daher wesentlich daran, ob sie unterschiedliche Lernvoraussetzungen nicht nur toleriert, sondern didaktisch produktiv verarbeitet.

3.12.4 Nutzung der Indikatoren für die Evaluierung

das Zusammenwirken von Wissensaufbau, Handlungskompetenz, prozessualer Sicherheit, organisatorischer Einbettung und didaktischer Umsetzung. Die Evaluierung erfüllt damit nicht nur eine prüfende Funktion, sondern auch eine qualitätssichernde und entwicklungsorientierte Funktion innerhalb des Gesamtprogramms. Sie schafft die Voraussetzung dafür, Lernergebnisse nachvollziehbar zu erfassen, Defizite im Ausbildungsdesign sichtbar zu machen und daraus gezielte Verbesserungsmaßnahmen abzuleiten.

Die Erhebung erfolgt über ein Bündel komplementärer Verfahren, um unterschiedliche Dimensionen von Ausbildungserfolg angemessen abzubilden. Dazu zählen Vorabtests zur Erfassung des Ausgangsniveaus, Beobachtungsbögen in praktischen Übungen, die Auswertung von Incident-Dokumentationen, standardisierte Feedbackbögen sowie Abschlussbewertungen auf

Modul- oder Programmebene. Diese Kombination aus diagnostischen, beobachtungsbasierten, dokumentationsanalytischen und subjektiv-evaluativen Verfahren ist deshalb sinnvoll, weil sie sowohl deklaratives Wissen als auch anwendungsbezogene Handlungskompetenz, Prozesssicherheit und subjektive Wahrnehmungen der Teilnehmenden erfasst. Im Deliverable wird ausdrücklich empfohlen, zu Beginn bestimmter Module eine kurze Überprüfung bereits vorhandener Kenntnisse durchzuführen und die Überprüfung der Lehrinhalte sowohl über schriftliche Prüfungen als auch über praktische Übungen abzubilden. Daraus lässt sich ableiten, dass die Evaluierung bewusst nicht auf ein einzelnes Messinstrument reduziert werden sollte, sondern als mehrperspektivisches Verfahren angelegt sein muss. Methodisch betrachtet verbindet dieses Evaluierungskonzept formative und summative Elemente. Formative Evaluierungsanteile dienen dazu, Lernprozesse bereits während der Ausbildung sichtbar zu machen und gegebenenfalls nachzusteuern. Dazu gehören insbesondere Vorabtests, laufende Beobachtungen in Übungen und qualitative Rückmeldungen durch Trainerinnen und Trainer. Summative Elemente hingegen zielen auf die abschließende Bewertung der Zielerreichung ab und umfassen insbesondere Modulabschlüsse, Abschlussübungen und die Gesamtbewertung des Curriculums. Im militärischen Ausbildungskontext ist diese Verbindung von formativer und summativer Evaluierung besonders relevant, da operative Handlungskompetenz sich nicht allein in einer Abschlussprüfung abbilden lässt, sondern schrittweise aufgebaut, beobachtet und reflektiert werden muss. Gerade bei heterogenen Zielgruppen und praxisorientierten Übungsformaten ist es daher erforderlich, Lernstände nicht nur am Ende, sondern auch während des Ausbildungsprozesses systematisch zu erfassen.

Die Evaluierung soll sowohl auf Ebene der Teilnehmenden als auch auf Ebene des Ausbildungsdesigns sowie der Trainerinnen und Trainer erfolgen. Auf Ebene der Teilnehmenden steht die Frage im Vordergrund, ob die definierten Lernziele tatsächlich erreicht werden, also ob sicherheitsrelevante Ereignisse erkannt, erste Analysen durchgeführt, Dokumentationen erstellt und regelkonforme Erstmaßnahmen eingeleitet werden können. Auf Ebene des Ausbildungsdesigns wird hingegen bewertet, ob Aufbau, Progression, Schwierigkeitsgrad, Übungsarchitektur und organisatorische Einbettung geeignet sind, diese Kompetenzen wirksam zu fördern. Auf Ebene der Trainerinnen und Trainer ist schließlich zu prüfen, ob Briefing, Begleitung, Feedback und Debriefing didaktisch konsistent und zielgruppenadäquat umgesetzt werden. Diese mehrstufige Betrachtung entspricht den Ergebnissen der Bedarfserhebung, in der sowohl fachliche Anforderungen, didaktische Anforderungen als auch Erwartungen an die Qualität der Lernbegleitung klar benannt wurden.

Ein besonderer Stellenwert kommt in diesem Zusammenhang den praktischen Übungen zu, da diese im militärischen SOC-/NOC-Kontext die zentrale Brücke zwischen Wissensvermittlung und operativer Anwendungsfähigkeit bilden. Die Evaluierung praktischer Übungen sollte daher nicht allein auf das Endergebnis oder die korrekte Lösung technischer Aufgaben fokussieren, sondern auch prozessuale Merkmale wie Kommunikation, Rollenverständnis, Eskalationsverhalten, Dokumentationsqualität und Einhaltung definierter Abläufe erfassen. Das Deliverable betont mehrfach, dass militärische Ausbildungsziele nicht durch rein technische Challenge-Formate erreicht werden, sondern Übungsszenarien erfordern, in denen auch Teamarbeit, Meldekettens, Reaktionsprozesse und Entscheidungsfindung unter Zeitdruck trainiert werden. Entsprechend sollten Beobachtungsbögen und Bewertungslogiken so gestaltet sein, dass sie diese sozio-technischen Aspekte systematisch berücksichtigen. Auch das im Dokument beschriebene Scoring in Trainingsumgebungen verweist darauf, dass für militärische Ausbildungsziele nicht reines Punktesammeln entscheidend ist, sondern eine Bewertung, die auch Prozessqualität, Kommunikation, Dokumentation und Rolleneinhaltung einbezieht. Die Auswertung von Incident-Dokumentationen stellt innerhalb des Evaluierungskonzepts ein besonders wertvolles Instrument dar, da sie eine Schnittstelle zwischen technischer Beobachtung, organisatorischer Verarbeitung und individueller Handlungskompetenz bildet. Dokumentationen machen nachvollziehbar, ob

Teilnehmende sicherheitsrelevante Vorfälle in strukturierter Form erfassen, priorisieren und an zuständige Stellen weitergeben können. Sie erlauben damit nicht nur eine Bewertung inhaltlicher Richtigkeit, sondern auch eine Einschätzung der Anschlussfähigkeit an nachgelagerte Reaktions- und Eskalationsprozesse. Aus didaktischer Sicht ist dies besonders bedeutsam, da gerade im militärischen Einsatzkontext strukturierte Weitergabe und nachvollziehbare Lagebeschreibung zentrale Voraussetzungen für wirksames Incident Handling darstellen. Die Analyse solcher Dokumentationen sollte daher als fester Bestandteil der Evaluierung verankert werden.

Ergänzend dazu liefern standardisierte Feedbackbögen wichtige Informationen über die subjektive Wahrnehmung des Ausbildungsprozesses. Diese erfassen etwa die Verständlichkeit der Inhalte, die Passung des Schwierigkeitsniveaus, die wahrgenommene Relevanz der Szenarien, die Qualität der Lernbegleitung sowie den Nutzen des erhaltenen Feedbacks. Solche subjektiven Bewertungen ersetzen keine leistungsbezogenen Messungen, sie ergänzen diese jedoch um eine Perspektive, die für die Weiterentwicklung didaktischer Settings unverzichtbar ist. Im Deliverable wurde deutlich, dass Teilnehmende insbesondere praxisnahe und realistische Übungsformate als relevant und motivierend wahrnahmen, gleichzeitig jedoch eine stärkere theoretische Vorbereitung und ein strukturierteres Onboarding vor praktischen Übungen einforderten. Daraus folgt, dass Feedbackdaten nicht nur als Zufriedenheitsmessung verstanden werden sollten, sondern als diagnostische Hinweise auf strukturelle Stärken und Schwächen des Curriculums. Für die Bewertung auf Ebene des Ausbildungsdesigns ist außerdem zu berücksichtigen, dass Evaluierung nicht nur lernzielbezogen, sondern auch curricular-reflexiv verstanden werden sollte. Sie dient damit der Überprüfung, ob die inhaltliche Auswahl, die Abfolge der Module, der Anteil theoretischer und praktischer Elemente sowie die eingesetzten Trainingsplattformen den Anforderungen der Zielgruppe und des militärischen Kontexts entsprechen. Das Deliverable weist darauf hin, dass die Ausbildungsunterlagen in regelmäßigen Abständen überprüft und aktualisiert werden sollen; als Richtwert wird eine Evaluierung alle zwei bis fünf Jahre genannt. Diese Periodisierung zeigt, dass Evaluierung nicht als einmalige Abschlussmaßnahme, sondern als Bestandteil eines kontinuierlichen Verbesserungsprozesses verstanden wird. Ein wissenschaftlich fundiertes Ausbildungskonzept sollte daher kurzfristige Kurs- und Übungsevaluationen mit längerfristigen curricularen Reviews verbinden.

Auch die Trainerinnen- und Trainer-Ebene ist integraler Bestandteil der Evaluierung. Die Qualität eines Ausbildungsprogramms hängt wesentlich davon ab, ob fachliche Expertise, didaktische Kompetenz und konsistente Begleitung zusammenwirken. Im Deliverable wird hervorgehoben, dass Lehrpersonal verpflichtende pädagogische und didaktische Ausbildungen absolvieren muss und dass Teilnehmende von Trainerinnen und Trainern insbesondere Fachkompetenz, Praxiserfahrung, Geduld und konstruktives Feedback erwarten. Daraus ergibt sich, dass die Evaluierung nicht nur den Lernerfolg der Teilnehmenden, sondern auch die Qualität von Briefing, Unterstützung im Übungsprozess und Debriefing erfassen sollte. Dies ist insbesondere deshalb relevant, weil ein didaktisch uneinheitliches Vorgehen die Vergleichbarkeit von Leistungen erschwert und die Wirksamkeit der Ausbildung insgesamt beeinträchtigen kann. Die Ergebnisse dieser Evaluierung bilden die Grundlage für die Weiterentwicklung des Curriculums, die Anpassung einzelner Module sowie die Verbesserung des Trainerprogramms. Ihre Funktion besteht somit nicht nur in der retrospektiven Bewertung, sondern in der prospektiven Steuerung zukünftiger Ausbildungsmaßnahmen. Werden auf Basis der Evaluierung beispielsweise Defizite im Grundlagenwissen, im Verständnis organisatorischer Abläufe oder in der Handhabung technischer Werkzeuge sichtbar, können gezielt vorbereitende Module, didaktische Anpassungen oder neue Übungsformate entwickelt werden. Ebenso können Rückmeldungen zur Über- oder Unterforderung, zur Relevanz einzelner Inhalte oder zur Qualität des Debriefings genutzt werden, um das Curriculum zielgruppensensitiver und wirksamer zu gestalten. Evaluierung wird damit zu einem zentralen Instrument evidenzbasierter Curriculumentwicklung.

4 Trainingsumgebung

Die Bedarfsanalyse macht deutlich, welche Fähigkeiten, Rollenanforderungen und Rahmenbedingungen eine militärische Cyber-Ausbildung berücksichtigen muss. Die folgende Darstellung der Trainingsumgebung übersetzt diese Anforderungen in ein technisches und betriebliches Zielbild. Im Mittelpunkt steht die Frage, wie eine integrierte Plattform beschaffen sein muss, damit realitätsnahe, reproduzierbare und sicher betreibbare Trainingsformate für SOC- und NOC-nahe Aufgaben wirksam umgesetzt werden können.

4.1 Scope & Abgrenzung

Dieses Kapitel definiert den inhaltlichen Geltungsbereich der zu konzipierenden Trainingsplattform und grenzt ihn gegenüber benachbarten Themenfeldern ab. Ziel ist eine eindeutige, prüfbare Grundlage für den nachfolgenden Architekturentwurf [94], die Variantenbewertung und die Validierung. Der Scope richtet sich konsequent an den Bedarfen der vorgesehenen Zielgruppen aus und berücksichtigt die spezifischen Rahmenbedingungen eines hochsicheren, vorzugsweise vom Internet entkoppelten Betriebs.

Im Mittelpunkt steht eine integrierte Plattform, die unterschiedliche Trainingsformate für die Aus- und Weiterbildung in Security Operations Centers (SOC) und Network Operations Centers (NOC) konsistent bereitstellt. Der Begriff „Trainingsplattform“ umfasst dabei die Gesamtheit der technischen Mittel zur Planung, automatisierten Bereitstellung, Durchführung, Beobachtung und Nachbereitung von Übungen. Dazu zählen insbesondere funktionsfähige Cyber-Range-Szenarien, in denen komplexe, mehrschichtige IT-/OT-Umgebungen mit realitätsnahen Angriffs- und Verteidigungsabläufen aufgebaut werden, sowie praxisorientierte Hands-on-Formate, die sich an „Hack-The-Box“-artigen Übungen orientieren. Die Plattform muss beide Modalitäten gleichwertig unterstützen, sodass sowohl längere, szenariobasierte Trainings als auch fein granulare, auf einzelne Fähigkeiten zielende Challenges auf derselben technischen Basis betrieben werden können. Entscheidend ist dabei die Wiederverwendbarkeit und Versionierbarkeit von Szenarien, um Lernpfade modular zu kombinieren und reproduzierbar zu machen.

Für Trainer:innen sind dedizierte Steuerungs- und Orchestrierungsfunktionen im Scope. Diese umfassen die modellgestützte Definition und Parametrisierung von Übungsszenarien, die automatisierte Provisionierung und Dekommissionierung der benötigten Ressourcen, die Rundensteuerung (Start, Pause, Eskalation, Einspielen von Ereignissen), die Zuteilung von Teilnehmer:innen zu Ressourcen sowie die begleitende Beobachtbarkeit mittels Metriken, Logs und Traces. Ergänzend umfasst der Scope die kuratierte Verwaltung eines Szenarien-Katalogs mit eindeutigen Versionen, Metadaten (Lernziele, benötigte Ressourcen, Sicherheitsstufe) und Prüfmechanismen zur Qualitätssicherung. Die Plattform soll die Auswertung während und nach der Übung unterstützen (After-Action-Review), indem sie relevante Datenpunkte strukturiert erfasst, korreliert und in eine nachvollziehbare Lernstandsdiagnose überführt.

Ein zentrales Gestaltungsfeld im Scope sind Simulations- und Emulationsfähigkeiten. Die Plattform muss sowohl virtuelle Infrastrukturen (insbesondere Virtual Machines und virtuelle Netzsegmente) als auch netzwerknahe Emulationen und Protokollsimulationen bereitstellen können. Darüber hinaus ist die Integration realer Komponenten („Hardware-in-the-Loop“) anzulegen, um technologie-nahe Trainingssituationen zu ermöglichen, ohne die Integrität des Trainingsumfelds zu gefährden. Die Kombination aus Simulation, Emulation und ggf. punktueller Realintegration ist so zu gestalten, dass sie reproduzierbar, messbar und für Trainer:innen kontrollierbar bleibt. Aus architektonischer Sicht sind hierfür klare Schnittstellen, Adapter und Gateways zu definieren, die die Kopplung an reale Geräte kapseln und auditierbar machen.

Hinsichtlich der Betriebsumgebung ist die Plattform für einen Offline- bzw. Air-Gap-Betrieb zu konzipieren und im Scope verbindlich festzuschreiben, dass alle Kernfunktionen ohne permanente Internetanbindung voll nutzbar sein müssen. Wo Verbindungen nach außen technisch unumgänglich sind – etwa für zeitweilige Aktualisierungen, definierte Datenimporte oder die Kopplung mit einem zweiten, gleichartig gehärteten Standort – sind ausschließlich streng gesicherte, zeitlich und inhaltlich beschränkte und kryptographisch abgesicherte Verbindungen zulässig. Daraus folgt, dass Artefakte (z. B. VM-Images, Container-Images, Pakete, Konfigurationen) über geprüfte, signierte und lokal gespiegelt vorgehaltene Repositorien verfügbar zu machen sind und die gesamte Plattform konsequent einem „Everything-as-Code“-Ansatz folgt, um Nachvollziehbarkeit und Wiederholbarkeit sicherzustellen.

Der Scope schließt die Erarbeitung eines begründeten Technologievorschlags ausdrücklich ein. Dieser Technologievorschlag hat die Eignung von Virtualisierungs-, Orchestrierungs-, Observability-, Konfigurations- und Policy-Werkzeugen unter den genannten Rahmenbedingungen zu bewerten und in eine konsistente Zielarchitektur zu überführen. Maßgebliche Bewertungskriterien sind dabei Sicherheit (inkl. Härbarkeit und Lieferkettentransparenz), Offline-Tauglichkeit, Skalierbarkeit, Bedienbarkeit für Trainer:innen, Integrationsfähigkeit von Simulation/Emulation/Realgeräten sowie Betriebsaufwand und Lebenszykluskosten. Der Scope umfasst ferner die Formulierung von Architekturprinzipien (z. B. Segmentierung, minimale Vertrauensannahmen, signierte Artefakte, reproduzierbare Builds) sowie die Definition der für den Betrieb erforderlichen Rollen- und Rechtekonzepte (RBAC), ohne jedoch organisatorische Umstrukturierungen vorzugeben.

Nicht Gegenstand dieses Deliverables ist die Beschaffung im Sinne von Marktanalyse, Ausschreibung, Lizenzierung, Vertragsgestaltung oder die verbindliche Auswahl konkreter Produkte. Out of Scope sind ebenso betriebswirtschaftliche Beschaffungsprozesse, Lieferantenauswahl und die operative Inbetriebnahme im produktiven Umfeld. Gleichwohl ist zu erwarten, dass der Technologievorschlag produktnahe Optionen mitführt und Entscheidungsvorlagen so aufbereitet, dass eine spätere Beschaffung faktenbasiert erfolgen kann; die Entscheidung selbst liegt jedoch außerhalb des hier definierten Arbeitsumfangs.

Zur Präzisierung des Scopes gehören Annahmen und Randbedingungen, deren Einhaltung für die Validität des Architekturentwurfs erforderlich ist. Dazu zählen die Verfügbarkeit einer hinreichenden lokalen Infrastruktur (Rechen-, Speicher- und Netzressourcen) in der Trainingsumgebung, die Einrichtung eines lokalen Identitäts- und Schlüsselmanagements (z. B. PKI/CA) für einen vom Internet entkoppelten Betrieb, sowie die Bereitstellung getrennter Sicherheitszonen mit klaren Kontroll- und Übergabepunkten. Weiterhin wird angenommen, dass die am Trainingsbetrieb Beteiligten über die notwendigen Rollen und Berechtigungen verfügen und dass organisatorische Prozesse (z. B. Freigaben, Change- und Release-Management) so ausgestaltet sind, dass sie den Offline-Charakter nicht unterlaufen.

Die hier vorgenommene Abgrenzung stellt sicher, dass die Plattform auf ihre Kernfunktion – die robuste, sichere und reproduzierbare Bereitstellung praxisnaher SOC/NOC-Trainings – fokussiert bleibt. Durch die Kombination aus Cyber-Range-Szenarien und Hands-on-Übungen, die konsequente Ausrichtung auf Trainer-Orchestrierung und Beobachtbarkeit sowie die planerische Verankerung von Simulation, Emulation und Realintegration entsteht ein kohärenter, messbarer Gegenstand für den Architekturentwurf. Zugleich verhindert die klare Trennung zu Beschaffungs- und Produktentscheidungen eine Verwässerung des Ziels und bewahrt die methodische Strenge: Der Technologievorschlag liefert die fachliche und technische Entscheidungsgrundlage, ohne sie mit organisatorischen oder kommerziellen Zwängen zu vermischen. In Summe schafft diese Definition des Scopes die notwendige inhaltliche und prozessuale Klarheit, um die nachfolgenden Kapitel – insbesondere Anforderungen, Architekturvarianten und Validierung – zielgerichtet und nachvollziehbar zu erarbeiten.

4.2 Anforderungen & Qualitätsziele

Aufbauend auf der zuvor vorgenommenen inhaltlichen Abgrenzung der Trainingsumgebung ist im nächsten Schritt zu bestimmen, welche Anforderungen an die Plattform in funktionaler und qualitativer Hinsicht zu stellen sind. Ziel dieses Kapitels ist es, die in der Bedarfsanalyse identifizierten fachlichen, organisatorischen, didaktischen und infrastrukturellen Erfordernisse in ein konsistentes Anforderungsmodell für die Trainingsplattform zu überführen. Damit schafft das Kapitel die methodische und konzeptionelle Verbindung zwischen den empirisch erhobenen Bedarfen des Ausbildungsfeldes und den nachfolgenden Architekturentscheidungen. Im Zentrum steht somit nicht allein die Frage, welche Leistungen die Plattform bereitstellen muss, sondern ebenso, unter welchen Qualitätsbedingungen diese Leistungen im militärischen Ausbildungskontext als belastbar, sicher, reproduzierbar und didaktisch wirksam gelten können.

Die Ableitung der Anforderungen folgt dabei der Grundannahme, dass eine militärisch anschlussfähige Trainingsplattform nicht ausschließlich über ihren Funktionsumfang beschrieben werden kann. Vielmehr ist ihre Eignung erst dann hinreichend bestimmt, wenn funktionale Anforderungen und nicht-funktionale Qualitätsziele gemeinsam betrachtet werden. Funktionale Anforderungen beschreiben jene Leistungen, die für Planung, Bereitstellung, Durchführung, Beobachtung und Nachbereitung von Trainings, Übungen und Labs erforderlich sind. Nicht-funktionale Anforderungen präzisieren demgegenüber jene Qualitätsattribute, unter denen diese Leistungen erbracht werden müssen, etwa im Hinblick auf Sicherheit, Verfügbarkeit, Wartbarkeit, Erweiterbarkeit, Nachvollziehbarkeit oder Reproduzierbarkeit. Gerade unter den Bedingungen hochsicherer, teilweise vom Internet entkoppelter und organisatorisch sensibler Ausbildungsumgebungen ist diese doppelte Perspektive konzeptionell unverzichtbar. Methodisch stützt sich das Kapitel auf ein wissenschaftlich begründetes und zugleich anwendungsorientiertes Vorgehen. Ausgangspunkt ist die systematische Betrachtung der relevanten Stakeholder und Zielgruppen sowie ihrer jeweiligen Ziele, Aufgaben, Informationsbedarfe und Erfolgskriterien im Trainingsbetrieb. Auf dieser Grundlage werden Anforderungen nicht als bloße Sammlung technischer Wunschvorstellungen formuliert, sondern als nachvollziehbare, priorisierbare und überprüfbare Aussagen strukturiert. Die Übersetzung von Bedarfen in prüfbare Anforderungen dient dabei zugleich der späteren Validierung: Sie ermöglicht es, Architekturentscheidungen, Testplanung und Evidenzführung in einer gemeinsamen Logik zusammenzuführen und über die Requirements-Traceability-Matrix konsistent rückverfolgbar zu machen. Das Kapitel leistet damit einen zentralen Beitrag zur methodischen Strenge des Gesamtentwurfs, da es sicherstellt, dass die technische Konzeption der Trainingsplattform nicht isoliert, sondern aus Stakeholder-Bedarf, Qualitätszielen und Nachweislogik heraus entwickelt wird.

Die nachfolgenden Unterkapitel entfalten diese Logik schrittweise. Zunächst werden die relevanten Stakeholder und Zielgruppen der Plattform analysiert, um deren spezifische Perspektiven und Anforderungen transparent zu machen. Darauf aufbauend werden die funktionalen Anforderungen in strukturierter und tracebarer Form formuliert. Anschließend werden die nicht-funktionalen Anforderungen als Qualitätsattribute präzisiert und in überprüfbare Zielgrößen überführt. Abschließend wird mit der Traceability ein Rahmen etabliert, der die konsistente Verknüpfung von Stakeholder-Bedarf, Anforderung, Architekturbaustein und Nachweis sicherstellt. Das Kapitel bildet damit die normative Grundlage für die folgenden Architekturvarianten, den Variantenvergleich sowie die spätere Validierung der Trainingsplattform.

4.2.1 Stakeholder- und Zielgruppenanalyse

Dieses Kapitel identifiziert und charakterisiert die relevanten Stakeholder und Zielgruppen der Trainingsplattform und leitet daraus belastbare Anforderungen ab. Die Analyse dient dem Zweck, die späteren Architekturentscheidungen explizit an den Bedarfen der Beteiligten auszurichten und

diese Bedarfe rückverfolgbar in funktionale und nicht-funktionale Anforderungen zu überführen. Dabei wird der besondere Kontext eines militärischen, teilweise air-gapped betriebenen Systems berücksichtigt, in dem Nachvollziehbarkeit, Reproduzierbarkeit und Bedienbarkeit unter Sicherheits- und Verfügbarkeitsvorgaben im Vordergrund stehen.

Methodisches Vorgehen. Die Analyse folgt einem kombinierten, wissenschaftlich begründeten Vorgehensmodell: (1) In Anlehnung an ISO/IEC/IEEE 42010 werden zunächst Stakeholder und deren „Concerns“ systematisch erhoben und begrifflich geschärft; (2) für jede primäre Gruppe wird eine verdichtete Persona-Beschreibung erstellt, die Ziele, Aufgaben, Informationsbedarfe und Erfolgskriterien im Trainingskontext erfasst; (3) auf dieser Basis wird ein qualitatives Wirkmodell formuliert, das die Interaktionen während Planung, Durchführung und Auswertung von Übungen beschreibt; (4) abschließend erfolgt eine Einordnung in eine einfache Power-Interest-Matrix, um die Priorisierung in der weiteren Architekturarbeit zu fundieren. Die Datengrundlage speist sich aus den vorliegenden Domänenannahmen und projektspezifischen Randbedingungen; wo möglich, werden die abgeleiteten Bedürfnisse in messbare Qualitätsziele (z. B. Bereitstellungszeiten, Latenzbudgets, AAR-Vollständigkeit) überführt. Das Ergebnis sind überprüfbare, traceable Anforderungen statt bloßer Wunschlisten.

Primäre Stakeholder: Militärische Trainer:innen (inkl. Übungsleitung). Die Trainer:innen verfügen über einen Hintergrund in Informatik und nehmen eine Doppelfunktion ein: Sie planen und kuratieren Szenarien, und sie führen als Übungsleitung die Trainings operativ durch. Ihre Zielsetzung ist zweifach: Zum einen benötigen sie ein Mittel, um heterogene Formate, von komplexen Cyber-Range-Szenarien bis zu fokussierten Hands-on-Labs, reproduzierbar, sicher und zeitgerecht bereitzustellen; zum anderen müssen sie während der Durchführung fein granular steuern können (Start/Stop, Eskalationen, Einspielen synthetischer Events, Ressourcenallokation), ohne die technische Integrität des Übungsnetzes zu gefährden. Daraus resultieren konkrete Concerns: robuste und nachvollziehbare Orchestrierung ohne Internetabhängigkeit; eine Szenarien- und Übungssteuerung mit klaren, auditierbaren Zustandsübergängen; Telemetrie und Beobachtbarkeit, die sowohl operative Lagebilder als auch didaktisch nutzbare Kennzahlen (z. B. Ereignis-Timeline, Reaktionszeiten, Fehlerbilder) liefern; und eine After-Action-Review-Unterstützung, die Daten aus Simulation, Emulation und realen Komponenten korreliert. Nicht-funktional stehen Zuverlässigkeit und Wiederholbarkeit (Everything-as-Code, signierte Artefakte) sowie Bedienbarkeit im Vordergrund: Trainer:innen müssen in der Lage sein, binnen definierter Zeitvorgaben (etwa < 30 Minuten für ein Standard-Szenario) sichere, konsistente Umgebungen zu provisionieren und bei Störungen deterministisch auf einen bekannten Zustand zurückzukehren. In der Power-Interest-Matrix sind die Trainer:innen klar im Quadranten „hohe Macht/hohes Interesse“ verortet; sie prägen die funktionalen Kernanforderungen und sind zentrale Anspruchsgruppe für Usability und Betriebsabläufe.

Primäre Zielgruppen: Auszubildende – Offiziere. Die Offiziersauszubildenden, mit Studienabschluss an der Theresianischen Militärakademie (Schwerpunkt Informatik), bringen fundierte theoretische Kenntnisse und die Erwartung an methodische Tiefe mit. Sie benötigen realitätsnahe, aber kontrollierte Umgebungen, in denen sie komplexe SOC-Aufgaben in Teams einüben können: von der Sensorik- und Logikette über Erkennung und Triage bis zu Koordination, Kommunikation und Eskalation. Wichtige Concerns sind eine ausreichende Komplexität und Varianz der Szenarien (inkl. „Fog-of-War“), transparente, messbare Lernfortschritte sowie die Möglichkeit, Hypothesen iterativ zu prüfen (z. B. durch definierte Replay-/Rollback-Fähigkeiten). Nicht-funktional stehen Konsistenz und Erklärbarkeit im Vordergrund: Artefakte und Ereignisse müssen so dokumentiert sein, dass Entscheidungen im AAR nachvollziehbar und reproduzierbar sind. In der Power-Interest-Matrix liegen Offiziere bei hohem Interesse und mittlerer Macht: Sie beeinflussen die didaktische Wirksamkeit, verfügen aber nicht über die direkte Steuerungshoheit der Plattform.

Primäre Zielgruppen: Auszubildende – Unteroffiziere. Die Unteroffiziere sind technisch affin, ihre formale Vorbildung ist jedoch heterogener. Für diese Gruppe ist ein stärker gestuftes, kompetenzbasiertes Vorgehen wesentlich: geführte Labs mit klaren Lernzielen, progressive Schwierigkeitsgrade, unmittelbares, verständliches Feedback und sichere „Fehlschlag-Räume“, in denen Handlungsalternativen gefahrlos ausprobiert werden können. Wichtige Concerns sind eine robuste, latenzarme Interaktion mit den Übungsressourcen (Clients, Konsolen, Dashboards), eine verlässliche Isolierung zwischen Gruppen sowie eine klare Sichtbarkeit des eigenen Lernfortschritts. Nicht-funktional stehen hier Stabilität und Barrierefreiheit im Vordergrund: Die Plattform muss Lastspitzen (z. B. viele parallele Hands-on-Instanzen) ohne spürbare Degradation abfangen und dabei eine einheitliche, kognitiv wenig belastende Bedienoberfläche bieten. In der Power-Interest-Matrix verorten sich Unteroffiziere bei hohem Interesse und geringerer Macht; sie sind damit eine Gruppe, für die Stellvertreterbedarfe (über Trainer:innen) besonders ernst zu nehmen sind.

Sekundäre Randbedingungen und implizite Anspruchsgruppen. Auch wenn ausdrücklich keine Sicherheitsbeauftragten als Stakeholder vorgesehen sind, ergeben sich aus dem militärischen Kontext nicht-funktionale Querschnittsanforderungen: Segmentierung, Minimalitätsprinzip, lückenlose Auditierbarkeit und Offline-Tauglichkeit. Diese Anforderungen sind nicht als zusätzliche Stakeholder zu verstehen, sondern als normative Rahmenbedingungen, die sich in Architekturprinzipien (z. B. Zero-Trust-Segmente, signierte Artefakte, reproduzierbare Builds, rollenbasierte Zugriffskontrolle) materialisieren müssen. Die Übungsleitung liegt bei den Trainer:innen; ein separates Operations- oder Security-Rollenmodell kann daher schlank gehalten werden, solange Governance-Anforderungen technisch verankert sind (Policies-as-Code, vordefinierte Change-Pfadmodelle, kontrollierte Release-Fenster).

Implikationen für die Architektur. Aus Sicht der Trainer:innen erfordert die Plattform eine leistungsfähige Übungs- und Szenariensteuerung mit deklarativen Szenariobeschreibungen, deterministischen Provisionierungsabläufen und umfassender Observability – alles ohne dauerhafte Internetabhängigkeit. Für die Offiziersauszubildenden muss die Plattform komplexe, förderbare Cyber-Range-Szenarien ebenso unterstützen wie gezielte Experimentiermöglichkeiten mit klarer AAR-Unterstützung. Für die Unteroffiziere sind zeitnahe Bereitstellung, guided Labs und stabile, leicht bedienbare Interfaces entscheidend. Quer zu allen Gruppen stehen Anforderungen an Reproduzierbarkeit, Isolierung und Messbarkeit: Artefakte sind offline vorzuhalten, Umgebungen als Code zu beschreiben, Lern- und Systemmetriken kontinuierlich und kontextualisiert zu erfassen. In Summe ergibt sich ein konsistentes Zielbild: eine modular aufgebaute, air-gap-fähige Trainingsplattform, die den Trainer:innen hohe Steuerungstiefe bietet, Offiziere und Unteroffiziere gemäß ihren unterschiedlichen Kompetenzprofilen wirksam adressiert und die didaktische Qualität über nachvollziehbare Daten absichert, ohne zusätzliche Stakeholderrollen jenseits der genannten Gruppen einzuführen.

4.2.2 Funktionale Anforderungen

Dieses Kapitel präzisiert die aus der Stakeholder- und Zielgruppenanalyse (4.2.1) abgeleiteten Bedarfe in Form prüfbarer, tracebarer Funktionsanforderungen. Ziel ist es, eindeutig zu bestimmen, was die Trainingsplattform leisten muss, ohne das wie der Umsetzung vorwegzunehmen. Der Fokus liegt auf den operativen Erfordernissen einer militärischen Ausbildungsumgebung für SOC- und NOC-Rollen, die unter Air-Gap-Bedingungen betrieben wird, förderierte Übungen unterstützt und sowohl Cyber-Range-Szenarien als auch Hands-on-Formate (HTB-artig) konsistent bereitstellt. Damit bildet dieses Kapitel die normative Grundlage für den Architekturentwurf, den Variantenvergleich und die Validierung im Testplan.

Methodisch werden die Anforderungen top-down aus den identifizierten Stakeholder-Zielen der Trainer:innen (inkl. Übungsleitung), der Offiziersauszubildenden (Informatikschwerpunkt) und der

technisch affinen Unteroffizier:innen abgeleitet und anschließend mit den Randbedingungen (Offline-Betrieb, Föderationsfähigkeit, Real-Integration) gespiegelt. Zur Priorisierung wird das MoSCoW-Schema [95] verwendet, um Muss-, Sollte- und Kann-Funktionen transparent gegeneinander abzugrenzen. Jede Anforderung wird mit Akzeptanzkriterien versehen, die im Sinne einer messbaren Verifikation (z. B. Bereitstellungszeiten, Latenzbudgets, Reproduzierbarkeit, AAR-Vollständigkeit) formuliert sind. Die Rückverfolgbarkeit wird über eine Requirements-Traceability-Matrix (Kapitel 4.2.4) sichergestellt, die für jede Anforderung die zugehörigen Architekturbausteine, Schnittstellen und Testfälle referenziert.

Inhaltlich gruppieren sich die Funktionsanforderungen entlang der zentralen Leistungsbereiche der Plattform: Szenarien- und Übungssteuerung (deklarative Beschreibungen, Orchestrierung, Rundenmanagement), Trainingsformate (komplexe Cyber-Ranges und geführte Hands-on-Labs mit Reset/Replay/Scoring), Simulation, Emulation und Real-Integration (VM-basierte Umgebungen, Netzwerk-/Protokoll-Emulation, Hardware-in-the-Loop), Föderierte Übungen (Multi-Site-Kopplung und interoperabler Datenaustausch), Offline-Artefaktversorgung (signierte Mirrors, SBOM), Provisionierung via IaC (Everything-as-Code, deterministische Rebuilds), Beobachtbarkeit und After-Action-Review (Telemetrie, Korrelation, reproduzierbare Replays), Rollen- und Rechteverwaltung (RBAC, Mandantentrennung), Ressourcen- und Kapazitätsmanagement sowie offene Schnittstellen und Erweiterbarkeit (APIs, Adapter-/Plugin-Modell). Durch diese strukturierte und priorisierte Definition entsteht eine belastbare Brücke zwischen pädagogischem Bedarf und technischer Realisierung, die es erlaubt, Architekturentscheidungen zielgerichtet und nachvollziehbar zu treffen. In der nachfolgenden Tabelle 2 werden die Ergebnisse konsolidiert beschrieben. Die Funktionen, priorisiert sie nach MoSCoW [95] und verankert sie mit messbaren Akzeptanzkriterien (AK) sowie einer Stakeholder-Zuordnung zur späteren Rückverfolgbarkeit (RTM).

TABELLE 2 FUNKTIONALE ANFORDERUNGEN

Kategorie	Anforderung (Titel)	Priorität	Stakeholder	Kurzbeschreibung	Akzeptanzkriterien (AK)
A. Szenarien- und Übungssteuerung	Szenarienkatalog & Versionierung	MUS S	[T]	Versionierter Katalog mit Metadaten (Lernziele, Ressourcen, Sicherheitsstufe).	Anlage, Duplizierung und Rollback ohne manuelle Nebenschritte; Version & Hash aller Artefakte protokolliert.
A. Szenarien- und Übungssteuerung	Deklarative Szenariobeschreibung	MUS S	[T]	Szenarien als „Everything-as-Code“ (Topologie, Rollen, Events, Bewertungslogik).	Parser validiert Modelle; fehlerhafte Beschreibungen mit Zeilenreferenz abgewiesen; erfolgreiche Provisionierung reproduzierbar $\geq 3\times$.
A. Szenarien- und Übungssteuerung	Orchestrierung & Laufzeitsteuerung	MUS S	[T]	Start/Stop/Pause, Eskalationen, Einspielen synthetischer	< 5 s Latenz zwischen Befehl und bestätigtem

Kategorie	Anforderung (Titel)	Priorität	Stakeholder	Kurzbeschreibung	Akzeptanzkriterien (AK)
				Events/Traffic, Zeitsteuerung.	Zustandsübergang; alle Übergänge auditierbar.
A. Szenarien- und Übungssteuerung	Runden-/Teilnehmermanagement	SOL LTE	[T,U,O]	Parallele Übungsrounden, Gruppenzuordnung, Ressourcen-Quotas.	≥ 10 parallele Runden ohne Ressourcenkonflikte; Isolation durch Netzrichtlinien-Checks nachweisbar.
B. Trainingsformate	Cyber-Range-Szenarien	MUS S	[T,O]	Mehrschichtige Übungsnetze (optional IT/OT) mit Blue/Red/Purple-Abläufen.	Bereitstellung eines Referenzszenarios in < 30 min; „Fog-of-War“-Parameter pro Run konfigurierbar.
B. Trainingsformate	Hands-on/HTB-artige Labs	MUS S	[U,O]	Kurzform-Challenges mit Reset/Replay, automatischem Scoring/Flag-Abnahme.	Vollständiger Reset < 60 s; Scoring-Ereignisse werden in AAR exportiert.
B. Trainingsformate	Guided Labs & Lernpfade	SOL LTE	[U]	Schrittweise Anleitungen, progressive Schwierigkeitsgrade, unmittelbares Feedback.	≥ 3 Schwierigkeitsstufen pro Lab; Feedback < 2 s nach Aktion.
C. Simulation, Emulation & Real-Integration	VM-basierte Infrastruktur	MUS S	[T]	Szenarien aus VMs/virtuellen Netzen; Snapshots/Clones steuerbar.	Snapshot-Erstellung < 120 s; Wiederherstellung auf „Known-Good“-State reproduzierbar.
C. Simulation, Emulation & Real-Integration	Netzwerk-/Protokoll-Emulation	SOL LTE	[T,O]	Emulation von Latenz/Jitter/Packet-Loss; Generatoren (NetFlow, Syslog, ICS/OT).	Parametrierung im Szenariomodell; Telemetrie erscheint im Monitoring binnen < 5 s.
C. Simulation, Emulation & Real-Integration	Hardware-in-the-Loop-Adapter	SOL LTE	[T]	Adapter/Gateways zur Anbindung realer Geräte bei strikter Isolation.	Positiv-/Negativ-Tests (kein Verkehr außerhalb definierter Guards);

Kategorie	Anforderung (Titel)	Priorität	Stakeholder	Kurzbeschreibung	Akzeptanzkriterien (AK)
					Ereignisse eindeutig als „Realquelle“ markiert.
D. Förderierte Übungen	Multi-Site-Föderation	MUS S	[T,O]	Durchführung über mehrere Standorte/Organisationen, Mandantentrennung.	Föderations-Handshake; Identitäts-/Schlüssel-Austausch; Namensraum-Isolierung; gemeinsame AAR-Timeline.
D. Förderierte Übungen	Interoperabilität der Übungsdaten	SOL LTE	[T]	Austausch standardisierter Telemetrie-/AAR-Pakete zwischen Sites.	Export/Import eines Runs ohne Informationsverlust; Prüfsumme/Signatur gültig.
E. Offline-/Air-Gap & Artefakte	Vollständige Offline-Funktion	MUS S	[T,U,O]	Alle Kernfunktionen ohne Internet; temporär nur streng gesicherte Links.	Disconnect-Test (≥ 24 h) ohne Funktionsverlust; Logs zeigen keine externen Abhängigkeiten.
E. Offline-/Air-Gap & Artefakte	Artefakt-Mirrors & Signaturen	MUS S	[T]	Lokale Repos für VM-/Container-Images & Pakete; Signaturprüfung/SBOM.	Manipulierte Artefakte deterministisch erkannt; SBOM exportierbar.
F. Provisionierung, IaC & Automatisierung	IaC-Provisionierung	MUS S	[T]	Szenarioerzeugung via IaC (Terraform/Ansible/Packer/Helm).	„Plan/Apply/Destroy“ erzeugt identische Resultate auf Referenz-HW; Drift-Detection verfügbar.
F. Provisionierung, IaC & Automatisierung	Golden Images & Rebuilds	SOL LTE	[T]	Reproduzierbare Builds der Basis-Images/Charts.	Vollständiger Rebuild aus Quell-Repo ohne Netzabhängigkeit erfolgreich.
G. Beobachtbarkeit & AAR	Telemetrie & Korrelation	MUS S	[T]	Zentrale Metriken, Logs, Events, Netzflüsse; Szenario-Zeitachse.	≥ 95 % der definierten Events korrekt zeitgestempelt; Korrelation pro Teilnehmer:in möglich.

Kategorie	Anforderung (Titel)	Priorität	Stakeholder	Kurzbeschreibung	Akzeptanzkriterien (AK)
G. Beobachtbarkeit & AAR	AAR-Berichte & Scoring	MUS S	[T,U,O]	Automatisch generierte AARs mit Replay, Artefaktanhängen, Score/KPI.	Export als signiertes Paket; Wiederabspielung kritischer Ereignisse deterministisch.
H. Nutzer-, Rollen- & Rechteverwaltung	RBAC & Mandantentrennung	MUS S	[T,U,O]	Rollen (Trainer:in/Übungsleitung, Teilnehmer:in, Beobachter:in); mandantenfähige Ressourcen.	Rechteprüfungen vor kritischen Aktionen; Cross-Tenant-Zugriffe technisch ausgeschlossen.
H. Nutzer-, Rollen- & Rechteverwaltung	Identitätsmanagement (offline-fähig)	SOL LTE	[T]	Lokale Identitäten/Token; Offline-CRLs/OCSP-Ersatzmechanismen.	Dokumentierter Token-Lebenszyklus; Ablauf/Rotation ohne Internet testbar.
I. Ressourcen-, Zeit- & Kapazitätsmanagement	Ressourcenplanung & Quotas	SOL LTE	[T]	Vorab-Checks für Compute/Storage/Netz; automatische Zuteilung/Pre-emption.	Start nur bei verfügbaren Mindestressourcen; klare Fehlermeldungen bei Engpässen.
I. Ressourcen-, Zeit- & Kapazitätsmanagement	Scheduling & Kalenderabgleich	KAN N	[T]	Planung/Reservierung von Hardware-Slots, Räumen, Zeitfenstern.	Konfliktfreie Planung ≥ 95 % bei konkurrierenden Anfragen.
J. Schnittstellen & Erweiterbarkeit	APIs für Automatisierung	MUS S	[T]	Versionierte, dokumentierte API (REST/gRPC) für Szenario, Orchestrierung, AAR.	OpenAPI/gRPC-Spec vorhanden; externer Integrations-Test erfolgreich.
J. Schnittstellen & Erweiterbarkeit	Plugin/Adapter-Modell	SOL LTE	[T]	Erweiterung um neue Sim-Engines/Realgeräte ohne Kernänderung.	Beispiel-Adapter implementiert; Heißtausch im Wartungsfenster möglich.
K. Daten- & Wissensmanagement	Lernstands-Tracking	SOL LTE	[U,O]	Ergebnisse/Badges je Person/Team; datenschutzkonform, offline.	Export persönlicher Lernverläufe; Anonymisierungsmodus für

Kategorie	Anforderung (Titel)	Priorität	Stakeholder	Kurzbeschreibung	Akzeptanzkriterien (AK)
					Statistik/Forschung.
K. Daten- & Wissensmanagement	Beispiel-/Referenzszenarien	KANN	[T]	Kuratierte Startkollektion für schnelle Inbetriebnahme.	„First Run“ (Referenzszenario) < 1 h ab jungfräulicher Installation.

Die Tabelle 2 formalisiert funktionale Anforderungen. Die Priorität folgt dem MoSCoW-Schema (MUSS = zwingend; SOLLTE = wichtig, wenn möglich; KANN = optional/nice-to-have). Stakeholder-Kürzel: [T] = Trainer:innen/Übungsleitung, [O] = Offiziersanwärter (Informatik), [U] = Unteroffiziere (technikaffin). Die Akzeptanzkriterien (AK) sind messbar formuliert (z. B. Zeitbudgets, Reproduzierbarkeit, Signaturprüfung) und dienen der Verifikation im Testplan. Jede Zeile ist für die Requirements-Traceability-Matrix (RTM) referenzierbar (Anforderung → Architekturbaustein → Testfall), um eine durchgängige Rückverfolgbarkeit von Stakeholder-Bedarf bis Nachweisführung sicherzustellen.

4.2.3 Nicht-funktionale Anforderungen (Qualitätsattribute)

In der nachfolgenden Tabelle 3 werden die nicht funktionalen Anforderungen präzisiert, inkludiert sind Qualitätsziele der Trainingsplattform und übersetzt in prüfbare, messbare Anforderungen. Die Formulierung folgt ISO/IEC/IEEE 42010 (Stakeholder-Concerns) und nutzt ein Attribute-Driven-Design (ADD) [96] mit ATAM-Szenarien [97], [98] (Stimulus → Kontext → Reaktion → Metrik), sodass jede Anforderung im Testplan verifiziert und in der RTM rückverfolgt werden kann. Der militärische Kontext (Air-Gap-Betrieb, föderierte Übungen, Real-Integration) bildet den normativen Rahmen.

TABELLE 3 NICHT-FUNKTIONALE ANFORDERUNGEN

Qualitätsattribut	Zielbild	Anforderungen (konsolidiert)	ATAM-Szenario (Stimulus/Kontext /Reaktion/Metrik)	Kennzahlen (Beispiele)
Sicherheit	Minimalitätsprinzip Zero-Trust-Segmente, nachweisbare Lieferkettensicherheit [9].	- Segmentierung & Least Privilege (Trennung von Management-/Übungs-/Föderationszonen) - Artefakt-Integrität: nur signierte Images/Packages inkl. SBOM - Kryptografie offline-tauglich (lokale PKI/CA, Offline-CRLs) - Unveränderliche, auditierbare Logs	Stimulus: Unsigned-Image wird eingebracht. Kontext: Air-Gap. Reaktion: Ablehnung, Alarm, Audit-Log. Metrik: < 2 s bis Ablehnung; Logeintrag mit Hash/Issuer.	Blockrate Signaturprüfung: 100 % Ablehnungszeit: < 2 s Vollständigkeit Audit-Log: 100 %
Verfügbarkeit & Zuverlässigkeit	Trainingsbetrieb bleibt auch bei Teilausfällen steuerbar.	- SLO Plattform-Core ≥ 99,5 % im Trainingszeitfenster - RTO ≤ 2 h (Dienste), RPO ≤ 15 min (Metadaten) - Fehlertoleranz: HA für	Stimulus: Compute-Node fällt während Übung aus. Kontext: Laufende Übung. Reaktion: Rescheduling ohne	SLO: ≥ 99,5 % RTO: ≤ 2 h RPO: ≤ 15 min



		Steuerung/Monitoring, Auto-Restart/Rescheduling	Datenverlust. Metrik: Wiederherstellung < 5 min.	
Leistungsfähigkeit & Skalierbarkeit	Deterministische Provisionierungs-/ Steuerungszeiten, elastische Skalierung.	- Orchestrierungs-Latenz < 5 s - Provisionierung Referenz-Szenario < 30 min; Reset < 60 s ≥ 10 parallele Runden ohne Ressourcenkonflikte	Stimulus: Gleichzeitiger Start von 10 Hands-on-Labs. Kontext: Peak-Last. Reaktion: Start innerhalb Budgets. Metrik: 95-Perzentil Startzeit ≤ 60 s.	Orchestrierungs-Latenz: < 5 s Provisionierung: < 30 min Reset: < 60 s
Mandantenfähigkeit & Isolation	Strikte Trennung zwischen Teams/Organisationen und Runs.	- Isolation auf Compute/Netz/Storage-Ebene (Namespaces/VRFs) - Policy-as-Code (Deny-by-Default) - Quotas pro Tenant/Run	Stimulus: Versuch eines Cross-Tenant-Zugriffs. Kontext: Mehrere parallele Runs. Reaktion: Block, Alarm, Audit-Nachweis. Metrik: 100 % Blockrate in Pen-Tests.	Cross-Tenant-Blocks: 100 % Policy-Compliance: 100 %
Bedienbarkeit & Operabilität	Geringe kognitive Last, deterministische Workflows (Trainer-Zentrierung).	- Häufige Aktionen (Start/Pause/Reset/AAR-Export) in ≤ 3 Interaktionen - Feedback/Fehlerursachen in < 2 s - Barrierearme Oberflächen, Rollen-Dashboards	Stimulus: Trainer:in pausiert ein Szenario. Kontext: Laufende Übung. Reaktion: Visuelles Feedback, Statuswechsel protokolliert. Metrik: Reaktionszeit ≤ 2 s.	Interaktionsschritte: ≤ 3 Feedback-Zeit: < 2 s
Beobachtbarkeit & Forensische Auswertbarkeit	Vollständige, korrelierte Sicht auf System- und Lernereignisse.	- MELT-Erfassung (Metrics, Events, Logs, Traces) - Globale Zeitbasis (offline-NTP/GPS), einheitliche Run-IDs - AAR-Replay	Stimulus: Rekonstruktion einer Eskalationskette. Kontext: Post-Run-Analyse. Reaktion: Korrelation & Replay. Metrik: ≥ 95 % Events korrekt zeitkorreliert.	Zeitkorrelation: ≥ 95 % Replay-Determinismus: nachweisbar
Änderbarkeit, Wartbarkeit & Skalierbarkeit	Schnelle, risikoarme Änderungen unter Air-Gap-Bedingungen.	- Everything-as-Code (IaC, Policies, Pipelines) - ADRs, semantische Versionierung	Stimulus: Update eines Adapters. Kontext: Staging-Umgebung offline.	Build-&-Deploy-Dauer: < 1 h Rollback-Erfolg: 100 %



Testbarkeit		• Offline Unit/Integrations/Compliance-Tests; MTDD/MTTR-Ziele	Reaktion: Build/Sign/Deploy, Rollback ohne Downtime. Metrik: Prozess < 1 h.	
Portabilität & Deployability	Betrieb auf gängigen Hypervisor/Bare-Metal-Stacks; keine harten Cloud-Bindungen.	• Dokumentierte Mindesthardware • Offline-Registry/Repos, reproduzierbare Builds (Packer) • Exportierbare „Site Packages“ (Images, Charts, Keys)	Stimulus: Verlagerung auf Ersatzhardware. Kontext: Air-Gap. Reaktion: Wiederinbetriebnahme Referenzszenario. Metrik: < 1 Arbeitstag.	Wiederinbetriebnahme: < 1 AT Build-Reproduzierbarkeit : nachweisbar
Interoperabilität & Förderationsfähigkeit	Standardisierte Kopplung zwischen Standorten/Organisationen.	• Standardprotokolle (z. B. HLA/DIS bzw. Gateways) • Stabile APIs (OpenAPI/gRPC) • Versionierte AAR/Telemetrieformate, mTLS, kurzlebige Keys	Stimulus: Föderierte Übung mit Partner-Site. Kontext: Getrennte Mandanten. Reaktion: Erfolgreicher Handshake, konsolidierte Timeline. Metrik: Keine Datenverluste, Isolation gewahrt.	Handshake-Erfolg: 100 % AAR-Konsistenz: 100 %
Datenschutz & Lernanalytik	Datenminimierung bei aussagekräftiger Lernstandsdiagnose.	• Pseudonymisierung/Anonymisierungsmodus • Konfigurierbare Aufbewahrungsfristen • Offline-Exports	Stimulus: AAR-Export im Anonymisierungsmodus. Kontext: Forschung/Statistik Reaktion: Keine personenbezogenen Felder, signiertes Paket. Metrik: Prüfsumme/Signatur gültig.	PII-Leaks: 0 Signatur-Validität: 100 %
Resilienz, Notfallvorsorge & Wiederanlauf	Geordnete Degradation statt harter Ausfälle.	• Runbooks (Failover, Backup/Restore) • Regelmäßige DR-Drills • Kapazitätspuffer ≥ 20 % während Trainingsfenstern	Stimulus: Ausfall der Observability-DB. Kontext: Laufende Trainings. Reaktion: Read-Only-AAR, Wiederherstellung der Telemetrie. Metrik: < 15 min.	DR-Drills: regelmäßig protokolliert Wiederherstellungszeit: < 15 min
Effizienz & Nachhaltigkeit	Ressourcenbewusster Betrieb ohne Qualitätseinbußen	• Ephemere Umgebungen, automatische	Stimulus: Inaktive Lab-Instanz ≥ 10 min.	Ressourceneinsparung: ≥ 50 %

		Stilllegung inaktiver Labs • Geteilte Golden-Images • Messung von Ressourcen-KPIs	Kontext: Ressourcenknappheit. Reaktion: Suspend/Freeze. Metrik: Einsparung CPU/RAM $\geq 50\%$ ggü. Idle.	Quote ephemerer Umgebungen: hoch

4.2.4 Traceability

Die Requirements Traceability Matrix (RTM) dient dazu, Anforderungen über den gesamten Lebenszyklus hinweg nachvollziehbar (traceable) zu machen. Sie verknüpft die im Dokument definierten Anforderungen mit ihren Ursprüngen (z. B. Stakeholder- bzw. Perspektivenbezug), der Priorisierung sowie den funktionalen Bausteinen bzw. Nachweisen, über die diese Anforderungen umgesetzt und überprüft werden. Damit stellt die RTM sicher, dass keine wesentlichen Anforderungen „verloren gehen“, doppelt interpretiert werden oder ohne klaren Umsetzungs- und Validierungsbezug bleiben.

In der nachfolgenden Tabelle sind die Anforderungen daher strukturiert abgebildet. Für jede Anforderung wird festgehalten:

- ID und Kurzbeschreibung der Anforderung (funktional oder nicht-funktional),
- die zugehörige Relevanz/Zuordnung (z. B. betroffene Stakeholdergruppen bzw. Perspektiven),
- die Priorität gemäß dem gewählten Priorisierungsschema,
- sowie die Zuordnung zu Use Cases, Architekturelementen oder Validierungs-/Testnachweisen, sofern bereits definiert.

Auf diese Weise ermöglicht die RTM sowohl eine vollständige Abdeckung der Anforderungen als auch eine gezielte Auswirkungsanalyse bei Änderungen: Wenn sich eine Anforderung oder ein Use Case ändert, kann unmittelbar nachvollzogen werden, welche weiteren Artefakte (z. B. Architekturentscheidungen, Schnittstellen, Testfälle) davon betroffen sind.

TABELLE 4 REQUIRMENTS TRACABILITY MATRIX (RTM)

Reql D	Kategorie / Attribute	Titel	Priorität	Stakehol der	Beschreibung	KPI	U C	Arc h A	Arc h B	Tes t Ca se	Status
FR - 01	A. Szenarien- und Übungssteuerung	Szenarienkatalog & Versionierung	MUSS	T	Versionierter Katalog mit Metadaten (Lernziele, Ressourcen, Sicherheitsstufe).	Anlage, Duplizierung und Rollback ohne manuelle Nebenschritte; Version & Hash aller Artefakte protokolliert.	U C- 01 , U C- 03				Nicht gestartet
FR - 02	A. Szenarien- und Übungssteuerung	Deklarative Szenariobeschreibung	MUSS	T	Szenarien als „Everything-as-Code“ (Topologie, Rollen, Events, Bewertungslogik).	Parser validiert Modelle; fehlerhafte Beschreibungen mit Zeilenreferenz abgewiesen; erfolgreiche Provisionierung reproduzierbar $\geq$ 3×.	U C- 01 , U C- 03				Nicht gestartet
FR - 03	A. Szenarien- und Übungssteuerung	Orchestrierung & Laufzeitsteuerung	MUSS	T	Start/Stop/Pause, Eskalationen, Einspielen synthetischer Events/Traffic, Zeitsteuerung.	< 5 s Latenz zwischen Befehl und bestätigtem Zustandsübergan g; alle Übergänge auditierbar.	U C- 01 , U C- 03				Nicht gestartet



Reql D	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
FR - 04	A. Szenarien- und Übungssteuerung	Runden- /Teilnehmermanagement	SOLLTE	T,U,O	Parallele Übungsrunden, Gruppenzuordnung, Ressourcen-Quotas.	≥ 10 parallele Runden ohne Ressourcenkonflikte; Isolation durch Netzrichtlinien-Checks nachweisbar.	U C-01 , U C-03				Nicht gestartet
FR - 05	B. Trainingsformate	Cyber-Range-Szenarien	MUSS	T,O	Mehrschichtige Übungsnetze (optional IT/OT) mit Blue/Red/Purple-Abläufen.	Bereitstellung eines Referenzszenarios in < 30 min; „Fog-of-War“-Parameter pro Run konfigurierbar.	U C-04				Nicht gestartet
FR - 06	B. Trainingsformate	Hands-on/HTB-artige Labs	MUSS	U,O	Kurzform-Challenges mit Reset/Replay, automatischem Scoring/Flag-Abnahme.	Vollständiger Reset < 60 s; Scoring-Ereignisse werden in AAR exportiert.	U C-04				Nicht gestartet
FR - 07	B. Trainingsformate	Guided Labs & Lernpfade	SOLLTE	U	Schrittweise Anleitungen, progressive Schwierigkeitsgrade, unmittelbares Feedback.	≥ 3 Schwierigkeitsstufen pro Lab; Feedback < 2 s nach Aktion.	U C-04				Nicht gestartet



Req ID	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
FR - 08	C. Simulation, Emulation & Real-Integration	VM-basierte Infrastruktur	MUSS	T	Szenarien aus VMs/virtuellen Netzen; Snapshots/Clones steuerbar.	Snapshot-Erstellung < 120 s; Wiederherstellung auf „Known-Good“-State reproduzierbar.	U C-06 , U C-04				Nicht gestartet
FR - 09	C. Simulation, Emulation & Real-Integration	Netzwerk-/Protokoll-Emulation	SOLLTE	T,O	Emulation von Latenz/Jitter/Packet-Loss; Generatoren (NetFlow, Syslog, ICS/OT).	Parametrierung im Szenariomodell; Telemetrie erscheint im Monitoring binnen < 5 s.	U C-06 , U C-04				Nicht gestartet
FR - 10	C. Simulation, Emulation & Real-Integration	Hardware-in-the-Loop-Adapter	SOLLTE	T	Adapter/Gateways zur Anbindung realer Geräte bei strikter Isolation.	Positiv-/Negativ-Tests (kein Verkehr außerhalb definierter Guards); Ereignisse eindeutig als „Realquelle“ markiert.	U C-06 , U C-04				Nicht gestartet



Req ID	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
FR - 11	D. Föderierte Übungen	Multi-Site-Föderation	MUSS	T,O	Durchführung über mehrere Standorte/Organisationen, Mandantentrennung.	Föderations-Handshake; Identitäts-/Schlüssel-Austausch; Namensraum-Isolierung; gemeinsame AAR-Timeline.	U C-05				Nicht gestartet
FR - 12	D. Föderierte Übungen	Interoperabilität der Übungsdaten	SOLLTE	T	Austausch standardisierter Telemetrie-/AAR-Pakete zwischen Sites.	Export/Import eines Runs ohne Informationsverlust; Prüfsumme/Signatur gültig.	U C-05				Nicht gestartet
FR - 13	E. Offline-/Air-Gap & Artefakte	Vollständige Offline-Funktion	MUSS	T,U,O	Alle Kernfunktionen ohne Internet; temporär nur streng gesicherte Links.	Disconnect-Test (≥ 24 h) ohne Funktionsverlust; Logs zeigen keine externen Abhängigkeiten.	U C-09 , U C-08				Nicht gestartet



Reql D	Kategorie / Attribute	Titel	Priorität	Stakehol der	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
FR - 14	E. Offline-/Air- Gap & Artefakte	Artefakt-Mirrors & Signaturen	MUSS	T	Lokale Repos für VM-/Container-Images & Pakete; Signaturprüfung/SBOM.	Manipulierte Artefakte deterministisch erkannt; SBOM exportierbar.	U C- 09 , U C- 08				Nicht gestartet
FR - 15	F. Provisionierung, IaC & Automatisierung	IaC-Provisionierung	MUSS	T	Szenarioerzeugung via IaC (Terraform/Ansible/Packer/Helm).	„Plan/Apply/Destr oy“ erzeugt identische Resultate auf Referenz-HW; Drift-Detection verfügbar.	U C- 02 , U C- 10				Nicht gestartet
FR - 16	F. Provisionierung, IaC & Automatisierung	Golden Images & Rebuilds	SOLLTE	T	Reproduzierbare Builds der Basis- Images/Charts.	Vollständiger Rebuild aus Quell- Repo ohne Netzabhängigkeit erfolgreich.	U C- 02 , U C- 10				Nicht gestartet
FR - 17	G. Beobachtbarkeit & AAR	Telemetrie & Korrelation	MUSS	T	Zentrale Metriken, Logs, Events, Netzflüsse; Szenario-Zeitachse.	≥ 95 % der definierten Events korrekt zeitgestempelt; Korrelation pro Teilnehmer:in möglich.	U C- 07 , U C- 08				Nicht gestartet



Req ID	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
FR - 18	G. Beobachtbarkeit & AAR	AAR-Berichte & Scoring	MUSS	T,U,O	Automatisch generierte AARs mit Replay, Artefaktanhängen, Score/KPI.	Export als signiertes Paket; Wiederabspielung kritischer Ereignisse deterministisch.	U C-07 , U C-08				Nicht gestartet
FR - 19	H. Nutzer-, Rollen- & Rechteverwaltung	RBAC & Mandantentrennung	MUSS	T,U,O	Rollen (Trainer:in/Übungsleitung, Teilnehmer:in, Beobachter:in); mandantenfähige Ressourcen.	Rechteprüfungen vor kritischen Aktionen; Cross-Tenant-Zugriffe technisch ausgeschlossen.	U C-01 – U C-10				Nicht gestartet
FR - 20	H. Nutzer-, Rollen- & Rechteverwaltung	Identitätsmanagement (offline-fähig)	SOLLTE	T	Lokale Identitäten/Token; Offline-CRLs/OCSP-Ersatzmechanismen.	Dokumentierter Token-Lebenszyklus; Ablauf/Rotation ohne Internet testbar.	U C-01 – U C-10				Nicht gestartet
FR - 21	I. Ressourcen-, Zeit- & Kapazitätsmanagement	Ressourcenplanung & Quotas	SOLLTE	T	Vorab-Checks für Compute/Storage/Netz; automatische Zuteilung/Pre-emption.	Start nur bei verfügbaren Mindestressourcen; klare Fehlermeldungen bei Engpässen.	U C-03 , U C-10				Nicht gestartet



Reql D	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
FR - 22	I. Ressourcen-, Zeit- & Kapazitätsmanagement	Scheduling & Kalenderabgleich	KANN	T	Planung/Reservierung von Hardware-Slots, Räumen, Zeitfenstern.	Konfliktfreie Planung $\geq 95\%$ bei konkurrierenden Anfragen.	U C-03 , U C-10				Nicht gestartet
FR - 23	J. Schnittstellen & Erweiterbarkeit	APIs für Automatisierung	MUSS	T	Versionierte, dokumentierte API (REST/gRPC) für Szenario, Orchestrierung, AAR.	OpenAPI/gRPC-Spec vorhanden; externer Integrations-Test erfolgreich.	U C-05 , U C-06 , U C-09				Nicht gestartet
FR - 24	J. Schnittstellen & Erweiterbarkeit	Plugin/Adapter-Modell	SOLLTE	T	Erweiterung um neue Sim-Engines/Realgeräte ohne Kernänderung.	Beispiel-Adapter implementiert; Heißtausch im Wartungsfenster möglich.	U C-05 , U C-06 , U C-09				Nicht gestartet



Req ID	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
FR - 25	K. Daten- & Wissensmanagement	Lernstands-Tracking	SOLLTE	U,O	Ergebnisse/Badges je Person/Team; datenschutzkonform, offline.	Export persönlicher Lernverläufe; Anonymisierungsmodus für Statistik/Forschung.	U C-07 , U C-08				Nicht gestartet
FR - 26	K. Daten- & Wissensmanagement	Beispiel-/Referenzszenarien	KANN	T	Kuratierte Startkollektion für schnelle Inbetriebnahme.	„First Run“ (Referenzszenario) < 1 h ab jungfräulicher Installation.	U C-07 , U C-08				Nicht gestartet
	Sicherheit	Minimalitätsprinzip, Zero-Trust-Segmente, nachweisbare Lieferkettensicherheit.	SOLLTE		- Segmentierung & Least Privilege (Trennung von Management-/Übungs-/Föderationszonen) - Artefakt-Integrität: nur signierte Images/Packages inkl. SBOM - Kryptografie offline-tauglich (lokale PKI/CA, Offline-CRLs) - Unveränderliche, auditierbare Logs	Stimulus: Unsigned-Image wird eingebracht. Kontext: Air-Gap. Reaktion: Ablehnung, Alarm, Audit-Log. Metrik: < 2 s bis Ablehnung; Logeintrag mit Hash/Issuer.	U C-01 – U C-10				Nicht gestartet



Req ID	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	UC	Arc h A	Arc h B	Test Case	Status
	Verfügbarkeit & Zuverlässigkeit	Trainingsbetrieb bleibt auch bei Teilausfällen steuerbar.	MUSS		- SLO Plattform-Core $\geq 99,5\%$ im Trainingszeitfenster $RTO \leq 2\text{ h}$ (Dienste), $RPO \leq 15\text{ min}$ (Metadaten) - Fehlertoleranz: HA für Steuerung/Monitoring, Auto-Restart/Rescheduling	Stimulus: Compute-Node fällt während Übung aus. Kontext: Laufende Übung. Reaktion: Rescheduling ohne Datenverlust. Metrik: Wiederherstellung $< 5\text{ min.}$	UC-01 – UC-10				Nicht gestartet
	Leistungsfähigkeit & Skalierbarkeit	Deterministische Provisionierungs-/Steuerungszeiten, elastische Skalierung.	KANN		- Orchestrierungs-Latenz $< 5\text{ s}$ - Provisionierung Referenz-Szenario $< 30\text{ min}$; Reset $< 60\text{ s}$ ≥ 10 parallele Runden ohne Ressourcenkonflikte	Stimulus: Gleichzeitiger Start von 10 Hands-on-Labs. Kontext: Peak-Last. Reaktion: Start innerhalb Budgets. Metrik: 95-Perzentil Startzeit $\leq 60\text{ s.}$	UC-01 – UC-10				Nicht gestartet



Reql D	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
	Mandantenfähigkeit & Isolation	Strikte Trennung zwischen Teams/Organisationen und Runs.	KANN		- Isolation auf Compute/Netz/Storage-Ebene (Namespaces/VRFs) - Policy-as-Code (Deny-by-Default) - Quotas pro Tenant/Run	Stimulus: Versuch eines Cross-Tenant-Zugriffs. Kontext: Mehrere parallele Runs. Reaktion: Block, Alarm, Audit-Nachweis. Metrik: 100 % Blockrate in Pen-Tests.	U C-01 – U C-10				Nicht gestartet
	Bedienbarkeit & Operabilität	Geringe kognitive Last, deterministische Workflows (Trainer-Zentrierung).	SOLLTE		- Häufige Aktionen (Start/Pause/Reset/AAR-Export) in ≤ 3 Interaktionen - Feedback/Fehlerursachen in < 2 s - Barrierearme Oberflächen, Rollen-Dashboards	Stimulus: Trainer:in pausiert ein Szenario. Kontext: Laufende Übung. Reaktion: Visuelles Feedback, Statuswechsel protokolliert. Metrik: Reaktionszeit ≤ 2 s.	U C-01 – U C-10				Nicht gestartet



Req ID	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
	Beobachtbarkeit & Forensische Auswertbarkeit	Vollständige, korrelierte Sicht auf System- und Lernereignisse.	SOLLTE		- MELT-Erfassung (Metrics, Events, Logs, Traces) - Globale Zeitbasis (offline-NTP/GPS), einheitliche Run-IDs - AAR-Replay	Stimulus: Rekonstruktion einer Eskalationskette. Kontext: Post-Run-Analyse Reaktion: Korrelation & Replay. Metrik: ≥ 95 % Events korrekt zeitkorreliert.	U C-01 – U C-10				Nicht gestartet
	Änderbarkeit, Wartbarkeit & Testbarkeit	Schnelle, risikoarme Änderungen unter Air-Gap-Bedingungen.	SOLLTE		- Everything-as-Code (IaC, Policies, Pipelines) - ADRs, semantische Versionierung - Offline Unit/Integrations/Compliance-Tests; MTTD/MTTR-Ziele	Stimulus: Update eines Adapters. Kontext: Staging-Umgebung offline. Reaktion: Build/Sign/Deploy, Rollback ohne Downtime. Metrik: Prozess < 1 h.	U C-01 – U C-10				Nicht gestartet



Reql D	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
	Portabilität & Deployability	Betrieb auf gängigen Hypervisor/Bare-Metal-Stacks; keine harten Cloud-Bindungen.	KANN		- Dokumentierte Mindesthardware - Offline-Registry/Repos, reproduzierbare Builds (Packer) - Exportierbare „Site Packages“ (Images, Charts, Keys)	Stimulus: Verlagerung auf Ersatzhardware. Kontext: Air-Gap. Reaktion: Wiederinbetriebnahme Referenzszenario. Metrik: < 1 Arbeitstag.	U C-01 – U C-10				Nicht gestartet
	Interoperabilität & Föderationsfähigkeit	Standardisierte Kopplung zwischen Standorten/Organisationen	KANN		- Standardprotokolle (z. B. HLA/DIS bzw. Gateways) - Stabile APIs (OpenAPI/gRPC) - Versionierte AAR/Telemetrieformate, mTLS, kurzlebige Keys	Stimulus: Föderierte Übung mit Partner-Site. Kontext: Getrennte Mandanten. Reaktion: Erfolgreicher Handshake, konsolidierte Timeline. Metrik: Keine Datenverluste, Isolation gewahrt.	U C-01 – U C-10				Nicht gestartet



Req ID	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	U C	Arc h A	Arc h B	Test Case	Status
	Datenschutz & Lernanalytik	Datenminimierung bei aussagekräftiger Lernstandsdiagnose.	KANN		- Pseudonymisierung/Anonymisierungsmodus - Konfigurierbare Aufbewahrungsfristen - Offline-Exports	Stimulus: AAR-Export im Anonymisierungsmodus. Kontext: Forschung/Statistik. Reaktion: Keine personenbezogenen Felder, signiertes Paket. Metrik: Prüfsumme/Signatur gültig.	U C-01 – U C-10				Nicht gestartet
	Resilienz, Notfallvorsorge & Wiederanlauf	Geordnete Degradation statt harter Ausfälle.	SOLLTE		- Runbooks (Failover, Backup/Restore) - Regelmäßige DR-Drills - Kapazitätspuffer ≥ 20 % während Trainingsfenstern	Stimulus: Ausfall der Observability-DB. Kontext: Laufende Trainings. Reaktion: Read-Only-AAR, Wiederherstellung der Telemetrie. Metrik: < 15 min.	U C-01 – U C-10				Nicht gestartet



Req ID	Kategorie / Attribute	Titel	Priorität	Stakeholder	Beschreibung	KPI	UC	Arc h A	Arc h B	Test Case	Status
	Effizienz & Nachhaltigkeit	Ressourcenbewusster Betrieb ohne Qualitätseinbußen	KANN		- Ephemere Umgebungen, automatische Stilllegung inaktiver Labs - Geteilte Golden-Images - Messung von Ressourcen-KPIs	Stimulus: Inaktive Lab-Instanz ≥ 10 min. Kontext: Ressourcenknappheit. Reaktion: Suspend/Freeze. Metrik: Einsparung CPU/RAM ≥ 50 % ggü. Idle.	UC-01 – UC-10				Nicht gestartet

4.3 Architekturleitlinien & Methodik

Dieses Kapitel definiert verbindliche Leitprinzipien und ein methodisches Vorgehensmodell für Entwurf, Bewertung und fortlaufende Weiterentwicklung der Trainingsplattform. Ziel ist eine konsistente, nachvollziehbare und prüfbare Architektur, die unter Air-Gap-Bedingungen betrieben werden kann, föderierte Übungen erlaubt und sowohl Cyber-Range-Szenarien als auch Hands-on-Formate effektiv unterstützt. Die Leitlinien bilden die Leitlinien für alle Design- und Betriebsentscheidungen; die Methodik beschreibt, wie Entscheidungen hergeleitet, dokumentiert, validiert und iterativ verbessert werden.

4.3.1 Zweck, Anwendungsbereich und Geltung

Die Leitlinien und Methoden gelten für alle Architekturartefakte der Plattform (Kontext-, Logik-, Daten-, Deployment-, Laufzeit-, Sicherheits-, Föderations- und Betriebs-Views) sowie für deren Lebenszyklus vom MVP bis zum produktionsnahen Trainingsbetrieb. Sie adressieren die Primärstakeholder Trainer:innen/Übungsleitung und die Zielgruppen Offiziers- und Unteroffiziersausbildung. Da keine separate Sicherheitsbeauftragtenrolle vorgesehen ist, werden Sicherheitsanforderungen technisch verankert (Policies-as-Code, Signaturen, Auditierbarkeit) und im Governance-Prozess verlässlich abgebildet.

4.3.2 Architekturleitlinien (Prinzipien)

P1 – Offline-First & Air-Gap-Tauglichkeit: Alle Kernfunktionen müssen ohne Internetverbindung vollumfänglich nutzbar sein. Aktualisierungen, föderierte Kopplungen oder Datenimporte erfolgen ausschließlich über zeitlich begrenzte, inhaltlich beschränkte, kryptografisch abgesicherte Verbindungen. Artefakte (VM-Images, Container-Images, Pakete) werden lokal gespiegelt und signiert vorgehalten. Implikation: Jede externe Abhängigkeit (z. B. NTP, Repos) erfordert einen lokalen, verifizierten Ersatz.

P2 – Security-by-Design & Zero-Trust-Segmente: Minimalitätsprinzip [100], strikte Segmentierung (Management-/Übungs-/Föderationszonen), rollenbasierte Kontrolle (RBAC) bis auf API-Operationsebene, durchgängig verschlüsselte Steuer- und Föderationskanäle, manipulationssichere Logs. Implikation: Standardzustand ist „deny-by-default“, Freigaben erfolgen policygesteuert und sind auditierbar.

P3 – Everything-as-Code & Reproduzierbarkeit: Szenarien (Topologien, Rollen, Events, Bewertungslogik), Infrastruktur, Policies, Pipelines und Dokumentations-Snippets sind als Code versioniert und signiert. Implikation: Deterministische Builds/Deploys (VM-Images, Charts), Rollback-Fähigkeit, reproduzierbare Tests.

P4 – Modularität, Austauschbarkeit & Komponentenneutralität

Kopplung zwischen Komponenten erfolgt über dokumentierte, stabile Schnittstellen (APIs, Event-/Sim-Standards); Module sind austauschbar. Implikation: Adapter/Plugin-Modell für Simulations-Engines und Realgeräte; klare „Ports & Adapters“-Grenzen.

P5 – Standards-First Interoperabilität

Für Simulations-/Föderationsanforderungen werden etablierte Standards bevorzugt (z. B. HLA/DIS sowie – wo sinnvoll – DDS-Bridges). Telemetrie und AAR folgen versionierten Austauschformaten. Implikation: Geringeres Integrationsrisiko in Multi-Site-Szenarien.

P6 – Beobachtbarkeit-by-Default & AAR-Tauglichkeit



Metriken, Logs, Events und Traces sind standardisiert erfassbar; alle Laufzeitaktionen sind zeitkorreliert und einer Run-ID zuordenbar. Implikation: AAR-Replay, Lernstandsdiagnose und forensische Nachvollziehbarkeit werden systemisch unterstützt.

P7 – Usability für Trainer:innen als Primärkriterium

Häufige Workflows (Start, Pause, Reset, Eskalation, AAR-Export) sind in ≤ 3 Interaktionen erreichbar, Rückmeldungen erfolgen < 2 s. Implikation: UI/UX-Entscheidungen werden anhand von Trainer-Journeys validiert.

P8 – Föderationsfähigkeit & Mandantentrennung

Architektur unterstützt sichere Kopplungen zwischen Standorten/Organisationen bei strikter Isolation von Namensräumen/VRFs und Daten. Implikation: mTLS-gesicherte Föderationslinks, kurzlebige Schlüssel, gemeinsame Timeline mit lokaler Souveränität.

P9 – Einfachheit vor Komplexität

Bei gleichwertigem Nutzen sind die robusteren und einfacheren Lösungen zu bevorzugen (KISS/Lean-Ops). Implikation: Minimierung optionaler Control-Plane-Abhängigkeiten, Reduktion „exotischer“ Komponenten.

P10 – Messbarkeit & Nachweisführung

Jede Anforderung erhält Metriken und Akzeptanzkriterien; Erfüllung wird im Testplan verifiziert und in AAR/Protokollen nachweisbar dokumentiert.

4.4 Kontext & Use-Cases

Dieses Kapitel beschreibt den Systemkontext und die zentralen Use-Cases der Trainingsplattform. Ziel ist die Ableitung prüfbarer Anforderungen, die sowohl die VM-zentrierte als auch die Kubernetes/Service-Mesh-Variante konsistent adressieren. Die Darstellung ist variantenneutral und bildet die Grundlage für Schnittstellen-, Test- und Sicherheitsentwurf.

4.4.1 Methodik

Die Kontext- und Use-Case-Analyse folgt einem kombinierten Rahmenwerk: (1) ISO/IEC/IEEE 42010 zur systematischen Erhebung von Stakeholdern und deren Concerns; (2) Goal-Oriented Requirements Engineering (GORE) [101] zur Ableitung von Zielen der Trainer:innen, Offiziers- und Unteroffiziersausbildung; (3) UML-Use-Case-Modellierung (strukturierte Steckbriefe) zur präzisen Beschreibung von Abläufen; (4) ATAM-Szenarien (Stimulus → Kontext → Reaktion → Metrik) zur Operationalisierung der Qualitätsattribute; (5) Attribute-Driven Design (ADD) als Entwurfstaktik, die Qualitätsziele in Architekturstrukturen überführt. Die Ergebnisse werden mit messbaren KPIs versehen und sind in der Requirements-Traceability-Matrix (RTM) referenzierbar.

4.4.2 Systemkontext

Akteur:innen: Trainer:innen/Übungsleitung (Orchestrierung, AAR), Offiziersauszubildende (komplexe Cyber-Range-Szenarien), Unteroffiziere (geführte Hands-on-Labs), optionale Beobachter:innen.

Plattform-Kern: Übungs-/Szenariensteuerung (Katalog, deklarative Modelle), Provisionierung (IaC), Simulations-/Emulationsdienste und Adapter (inkl. Hardware-in-the-Loop), Föderations-Gateway (sichere Multi-Site-Kopplung), Observability & AAR, Identität & RBAC (offline-fähig).

Externe Systeme: Artefakt-Spiegel (signierte VM/Container-Images, Pakete, SBOMs), lokale Zeitquelle (NTP/GPS), reale Geräte/Netzkomponenten über isolierte Adapter, Partner-Sites für föderierte Übungen (nur streng gesicherte Verbindungen).

Sicherheits-/Vertrauensgrenzen: Management-Zone, Übungs-/Szenario-Zonen (pro Run/Tenant), Föderations-Zone (Gateways/Guards, mTLS), Observability-Zone.

4.4.3 Domänenmodell

Das Domänenmodell der Trainingsplattform formalisiert die fachlichen Entitäten, deren Zustände und Relationen sowie die für einen reproduzierbaren, air-gap-fähigen Trainingsbetrieb notwendigen Invarianten. Es dient als semantische Grundlage für Architektur-, Schnittstellen- und Testentwurf und gewährleistet die Konsistenz zwischen Use-Cases, funktionalen und nicht-funktionalen Anforderungen sowie der Nachweisführung.

Zentrale Entität ist das Szenario als deklarative, versionierte und kryptografisch signierte Beschreibung eines Trainingsvorhabens. Ein Szenario umfasst (i) eine Topologie aus Hosts, Diensten, Netzen und Segmenten, (ii) Rollen der Beteiligten (z. B. Blue/Red/Purple-Team, Beobachter:innen), (iii) Ereignisse/Injects zur zeit- oder zustandsbasierten Beeinflussung der Übung (Angriffssequenzen, Störungen, IOC-Einspielungen) und (iv) eine Bewertungslogik, durch die Beobachtungen (Telemetrie, Aktionen von Teilnehmenden) in messbare Ergebnisse überführt werden. Szenarien werden als Everything-as-Code beschrieben. Es gilt die Invariante, dass jede Szenario-Version unveränderlich ist (Immutabilität) und über Hash und Signatur eindeutig referenziert wird; Änderungen erfolgen ausschließlich durch Erzeugung einer neuen Version.



Die operationale Instanz eines Szenarios wird als Runde (Run) modelliert. Ein Run instanziiert genau eine Szenario-Version in einem definierten Kontext aus Ressourcenbudget, Teilnehmer-/Rollen-Zuordnung und optionalem Föderationsstatus. Zur Gewährleistung der Wiederholbarkeit werden Runs mit einer global eindeutigen Run-ID versehen; sämtliche Laufzeitdaten referenzieren diese ID. Zustandsautomaten sichern den Lebenszyklus (geplant → provisioniert → laufend → pausiert → abgeschlossen → archiviert) ab. Ein Zustandsübergang in laufend ist nur zulässig, wenn (a) alle referenzierten Artefakte erfolgreich verifiziert wurden und (b) die geforderten Mindestressourcen (Compute/Storage/Netz) reserviert sind. Isolation wird durch dedizierte Namensräume/VRFs und Richtlinien (deny-by-default) hergestellt.

Artefakte sind deploybare Einheiten, insbesondere VM-Images, Container-Images, Charts und Pakete. Jedes Artefakt besitzt (i) eine Signatur und (ii) eine Software Bill of Materials (SBOM). Artefakte werden in lokalen Spiegeln vorgehalten, um Air-Gap-Betrieb zu ermöglichen. Referenzen auf Artefakte erfolgen inhaltlich adressiert (Digest/Hash). Es gilt: Artefaktimporte ohne gültige Signatur sind deterministisch zu verwerfen; der Verwerfungsakt ist zu auditieren.

Ereignisse/Injects bilden steuernde Stimuli. Zwischen geplanten Injects (Bestandteil des Szenarios) und ad-hoc-Eingriffen der Übungsleitung wird formal unterschieden. Beide werden über eine einheitliche Ereignisschnittstelle eingebracht; sie sind jedoch unterschiedlich zu kennzeichnen, um Reproduzierbarkeit und didaktische Attribution zu sichern. Ein Ereignis trägt mindestens Zeitbezug, Quelle (synthetisch vs. Realquelle), Zielobjekte und Semantik; ad-hoc-Eingriffe unterliegen denselben Audit- und Policy-Regeln wie geplante Injektionen.

Die Laufzeitbeobachtung erfolgt über Telemetrie im Sinne von MELT (Metrics, Events, Logs, Traces) inklusive Netzwerkflüssen und Scoring-Ereignissen. Alle Telemetriedaten sind Run-ID-gebunden; Zeitstempel basieren auf einer lokalen, vertrauenswürdigen Zeitquelle (z. B. NTP/GPS). Aus Telemetrie und Ereignisprotokollen wird ein AAR-Paket erzeugt, das die rekonstruierbare Zeitlinie, Artefakt- und Konfigurationsreferenzen, Score-/KPI-Aggregationen und optional anonymisierte Personenbezüge enthält. AAR-Pakete sind zu signieren; Referenzen (Checksummen, Hashes) müssen verifizierbar sein. Eine Verletzung der Zeitkonsistenz (z. B. Drift über Schwellwert) ist zu kennzeichnen.

Für Mehrstandortszenarien definiert das Modell den Föderationslink als kontrollierte Beziehung zwischen zwei souveränen Plattforminstanzen. Ein Föderationslink kapselt Trust-Anker (Zertifikate, Policies), die Abbildung von Namensräumen/VRFs sowie Regeln zur Datenminimierung (welche Telemetrie- und Steuersignale exportiert werden). Föderationslinks sind zweckgebunden und zeitbegrenzt; sie verfallen automatisch, wenn kein Run mehr aktiv ist oder der Schlüssel-Lebenszyklus endet. Es gilt die Invariante, dass lokale Mandantentrennung nicht verletzt werden darf; Cross-Tenant-Zugriffe sind kategorisch zu blockieren und zu alarmieren.

Identität und Rollen werden als eigenständige Domänenobjekte modelliert. Identitäten (Personen, Dienste) besitzen Credentials mit lokal verifizierbaren Gültigkeiten (Kurzzeittoken, Offline-CRLs). Rollen bündeln Rechte entlang der Aufgaben (Trainer:in/Übungsleitung, Teilnehmer:in, Beobachter:in) und wirken auf Ebene der zugänglichen Operationen der Management- und Orchestrierungs-APIs. Least-Privilege ist verpflichtend; besonders eingriffsintensive Operationen (Föderationsaufbau, HIL-Freischaltung) unterliegen einem dokumentierten Vier-Augen-Prinzip.

Der Szenariokatalog fungiert als fachlicher Index über Szenario-Versionen mitsamt Metadaten (Lernziele, Sicherheitsstufe, Ressourcenbedarf, Freigabestatus). Er ist Bestandteil der Governance: Nur freigegebene und signierte Szenario-Versionen sind instanzierbar. Depublikation wirkt prospektiv; bereits instanziierte oder archivierte Runs bleiben referenzierbar, wodurch die Reproduzierbarkeit von Ergebnissen gesichert bleibt.

Die Relationsstruktur folgt stabilen Kardinalitäten: Eine Szenario-Definition besitzt n Versionen; eine Version kann in m Runs instanziiert werden; ein Run referenziert k Artefakte und erzeugt viele Telemetrie- und Ereigniseinträge; ein AAR-Paket aggregiert eine Teilmenge dieser Einträge. Ein Föderationslink verbindet zwei Plattformen, kann jedoch mehrere gleichzeitige Runs transportieren, wobei jeder Run eine eigene Isolations- und Policy-Konfiguration mitführt. Diese Kardinalitäten werden in den Schnittstellen (z. B. REST/gRPC) durch stabile Ressourcenpfade, referenzielle Integrität (IDs, Hashes) und Validierungsregeln abgebildet.

Die Lebenszyklen der Aggregate sind explizit definiert. Szenario-Versionen entstehen über Validierungs- und Signaturpipelines und sind danach unveränderlich. Runs werden deterministisch aus Szenario-Versionen und Artefakten erzeugt; Endzustände sind eindeutig, und es verbleiben revisionssichere AAR-Artefakte. Föderationslinks werden explizit hergestellt, überwacht und mittels Ablauf- oder Revokationsereignissen widerrufen. Diese Lebenszyklen stellen fachliche Verträge dar, die Wiederholbarkeit, Auditierbarkeit und Prüfbarkeit im militärischen Trainingskontext gewährleisten.

4.4.4 Use-Case

Das Use-Casekapitel integriert die Übersicht (Tabelle 5) und Detailbeschreibungen in einem. Die Use-Cases sind aus Stakeholder-Bedarfen und den Anforderungsdefinitionen abgeleitet. Jede Instanz benennt Zielsetzung, Vorbedingungen, Hauptabläufe, Alternativen, Nachbedingungen und messbare KPIs; Bezüge zu Qualitätsattributen, Schnittstellen und Datenobjekten sind explizit aufgeführt.

TABELLE 5 USE CASE ÜBERSICHT

UC-ID	Titel	Primärakteur	Ziel / Ergebnis	Haupt-KPIs
UC-01	Szenario modellieren & versionieren	Trainer:in	Deklaratives Szenario anlegen, validieren, versionieren und freigeben.	Fehlermarkierung < 2 s; Re-Provisionierung $\geq 3\times$ identisch
UC-02	Szenario provisionieren (laC)	Trainer:in	Automatisierte Bereitstellung (VM/Netz/Container) inkl. Pre-Flight-Checks.	Standard-Range < 30 min; automatisches Rollback bei Fehler
UC-03	Übung starten/steuern	Übungsleitung	Start/Pause/Eskalation/Event-Injection; deterministische Zustandswechsel.	Orchestrierungs-Latenz < 5 s; ≥ 10 parallele Runden
UC-04	Hands-on-Lab absolvieren	Unteroffizier:in / Offizier:in	Durchführung eines geführten Labs/Challenge mit Scoring, Reset, Replay.	Reset < 60 s; Feedback < 2 s; ≥ 3 Schwierigkeitsstufen

UC-ID	Titel	Primärakteur	Ziel / Ergebnis	Haupt-KPIs
UC-05	Föderierte Übung koppeln	Trainer:in (Site-Admin)	Sichere Multi-Site-Kopplung mit Mandantentrennung und gemeinsamer Timeline.	Isolation 100 %; AAR-Timeline konsistent
UC-06	Realgerät anbinden (HIL)	Trainer:in	Adaptergestützte Integration realer Komponenten unter strikter Isolation.	Kein Verkehr außerhalb Guards; Events als „Realquelle“ markiert
UC-07	Observability & Triage	Trainer:in/Beobachter:in	Live-Sicht, Korrelation, KPI-Dashboards für didaktische Steuerung.	≥ 95 % Events zeitkorreliert; Query-Zeit < 2 s
UC-08	AAR erzeugen & exportieren	Trainer:in	Erzeugung eines signierten, reproduzierbaren AAR-Pakets mit Replay.	Deterministisches Replay; gültige Signatur/Prüfsumme
UC-09	Artefakt-Supply offline	Plattform-Engineering / Trainer:in	Import/Update signierter Artefakte aus lokalen Spiegeln; Staging-->Prod.	100 % Signaturprüfung; Ablehnungszeit < 2 s
UC-10	Reset/Recovery/DR	Übungsleitung/Plattform-Ops	Geordnete Wiederherstellung (Run-Reset, Service-Failover, DR-Drill).	Reset < 60 s; Observability-Wiederherstellung < 15 min

UC-01 – Szenario modellieren & versionieren

Dieser Anwendungsfall beschreibt die formale Erzeugung und Pflege einer Szenario-Definition als deklaratives, versioniertes und kryptografisch signiertes Artefakt. Ausgangslage sind vorhandene Schreibrechte der Trainer:innen, erreichbare lokale Artefakt-Spiegel sowie kuratierte Vorlagen. Der Prozess beginnt mit der Ableitung eines neuen Repositoriums aus einer referenzierten Vorlage und der Erstellung der Szenariobeschreibung als „Everything-as-Code“ (Topologie, Rollen, Ereignisse/Injektionen, Bewertungslogik). Eine schematische und syntaktische Validierung identifiziert Fehler deterministisch und verweist mit Zeilenreferenzen; erst eine fehlerfreie Beschreibung wird signiert, mit Metadaten (Lernziele, Ressourcenprofil, Sicherheitsstufe) versehen und versioniert. Die Freigabe in den Katalog erfolgt im Vier-Augen-Prinzip und ist vollständig auditierbar. Fehlende Artefakte werden nicht implizit nachgeladen, sondern über einen expliziten Import mit Signatur-/SBOM-Prüfung eingebracht. Qualitätskriterien sind eine Fehlermarkierung < 2 s sowie die Re-Provisionierbarkeit ≥ 3× identisch. Der Use-Case realisiert Anforderungen an Sicherheit (Integrität/Authentizität durch Signaturen), Wartbarkeit und Nachvollziehbarkeit (Versionierung, Immutabilität) sowie Usability (präzise Fehlerrückmeldungen).

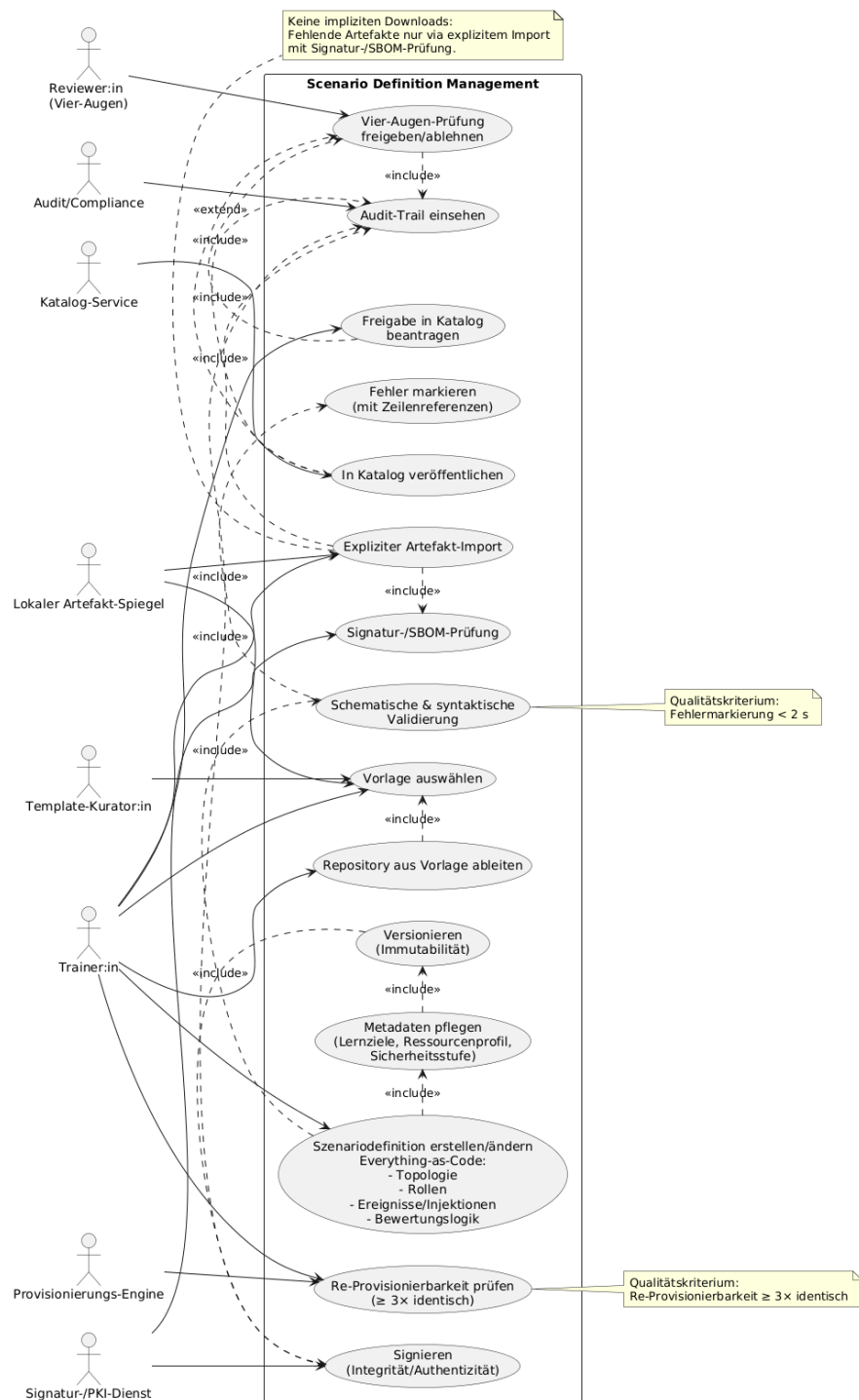


ABBILDUNG 5 SZENARIO MODELLIEREN & VERSIONIEREN

UC-02 – Szenario provisionieren (laC)

Ziel ist die deterministische Bereitstellung einer lauffähigen Übungsumgebung auf Basis einer freigegebenen Szenario-Version. Vorausgesetzt werden verfügbare Ressourcen, verifizierte Artefakte und definierte Quotas. Der Ablauf umfasst Pre-Flight-Checks (Signaturen, Kompatibilität, Kapazität), das Ausführen einer Plan/Apply-Pipeline (VM-, Netz-, ggf. Container-Ressourcen) und anschließende Health-Checks mit Übergabe an die Orchestrierung. Jeder Schritt ist transaktional und auditierbar; Fehler in Apply führen zu automatischem Rollback auf einen bekannten Zustand,

Ressourcenknappheit zu einem begründeten, reproduzierbaren Abbruch. Als Leistungsziel gilt für ein Referenzszenario eine Bereitstellungszeit < 30 min; Drift-Detection ist aktiv. Der Use-Case operationalisiert Performance- und Zuverlässigkeitsziele und stützt die Testbarkeit durch deterministische Build-/Deploy-Pfade.

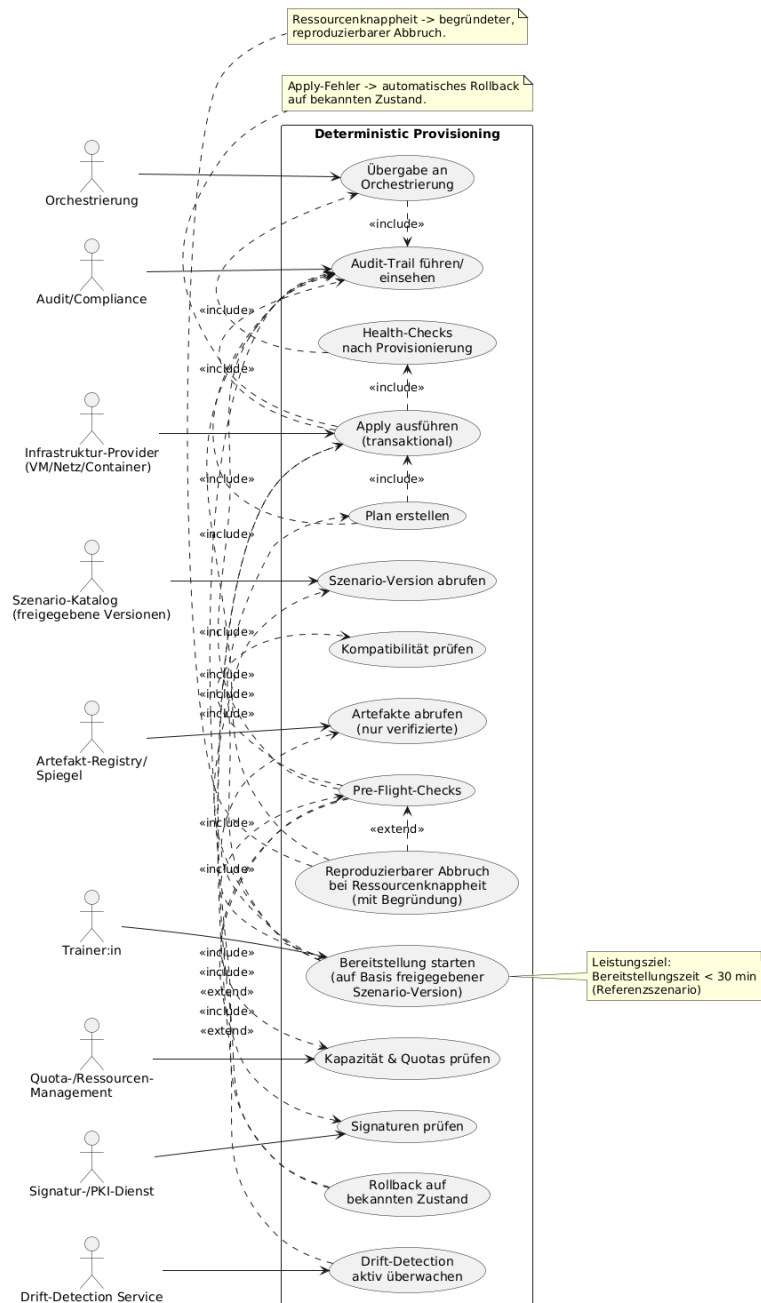


ABBILDUNG 6 SZENARIO PROVISIONIEREN (IAC)

UC-03 – Übung starten/steuern

Die Übungsleitung initiiert den Run zeit- oder ereignisgesteuert, nachdem UC-02 erfolgreich war und die Teilnehmenden zugeordnet sind. Die Orchestrierung übernimmt Start, Pause/Resume, Eskalationen und Event-Injection; begleitende Konsistenz- und Isolationsprüfungen stellen die Einhaltung von Mandantengrenzen und Richtlinien sicher. Alle Zustandsübergänge werden zeitgestempelt und der Run-ID zugeordnet. Fehlende Ressourcen erzwingen eine Neuplanung, Policy-Verstöße werden geblockt und alarmiert. Metrisch maßgeblich sind eine Orchestrierungs-

Latenz < 5 s sowie die Fähigkeit, mindestens zehn parallele Runden konfliktfrei zu führen. Der Use-Case verknüpft Usability-Vorgaben (Reaktionszeiten) mit Sicherheits- und Verfügbarkeitsanforderungen (Auditierbarkeit, robuste Steuerbarkeit).

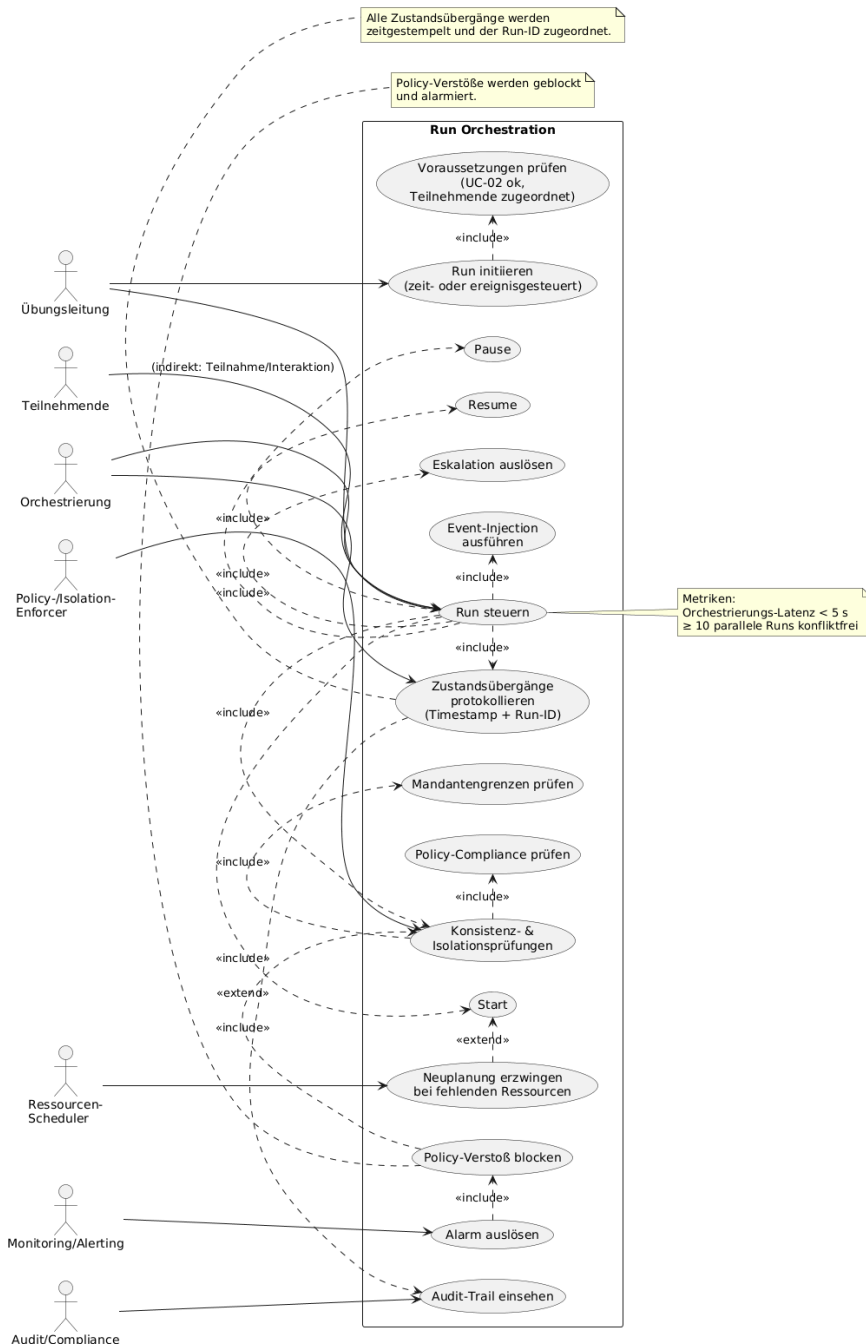


ABBILDUNG 7 ÜBUNG STARTEN/STEUERN

UC-04 – Hands-on-Lab absolvieren

Teilnehmende starten ein bereitgestelltes Lab aus dem Katalog und bearbeiten eine klar formulierte Aufgabenstellung mit optionalen, kontextsensitiven Hints. Ergebnisse werden über ein automatisiertes Scoring (z. B. Flag-Abnahme) erfasst; Reset/Replay-Funktionen erlauben kontrollierte Wiederholungen ohne Seiteneffekte. Instanzfehler lösen einen automatischen Reset aus; bei Fehlbedienung werden didaktisch motivierte Hinweise angeboten. Kennzahlen sind ein Reset < 60 s, Feedback < 2 s sowie mindestens drei Schwierigkeitsstufen je Lab. Der Use-Case

adressiert vorrangig Usability und Performance sowie die Beobachtbarkeit von Lernergebnissen (Scoring-Events als Telemetrie), unter strikter Isolierung der Tenant-/Run-Umgebung.

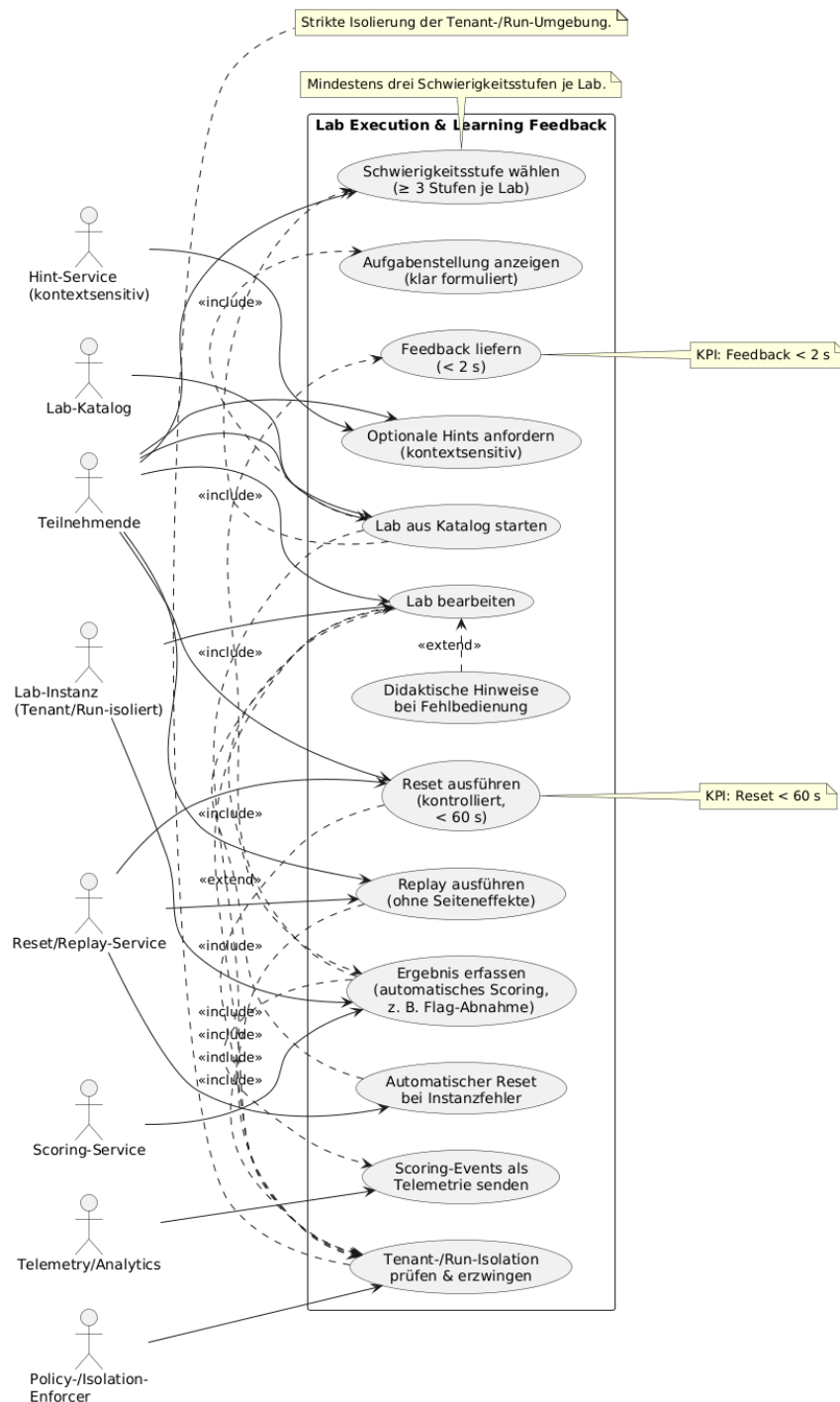


ABBILDUNG 8 HANDS-ON-LAB ABSOLVIEREN

UC-05 – Föderierte Übung koppeln

Zwei souveräne Plattforminstanzen verbinden sich für eine gemeinsame Übung über einen kontrollierten Föderationslink. Voraussetzungen sind gegenseitige Trust-Anker und ein freigegebener, minimaler Netzpfad. Der Kopplungsprozess umfasst einen mTLS-Handshake mit kurzlebigen Schlüsseln, die Etablierung einer Namensraum-/VRF-Isolation, den Austausch minimaler Steuer-/Telemetriedaten sowie die Vergabe einer gemeinsamen Run-ID/Timeline.

Timeline-Drift wird erkannt und korrigiert; scheitert der Handshake, erfolgt ein definierter Abbruch ohne Partial-Trust. Qualitätsziele sind eine nachweislich vollständige Isolation (100 %) und eine konsistente AAR-Zeitachse. Der Use-Case konkretisiert Interoperabilitäts-, Sicherheits- und Zeitkonsistenzanforderungen im Multi-Site-Betrieb.

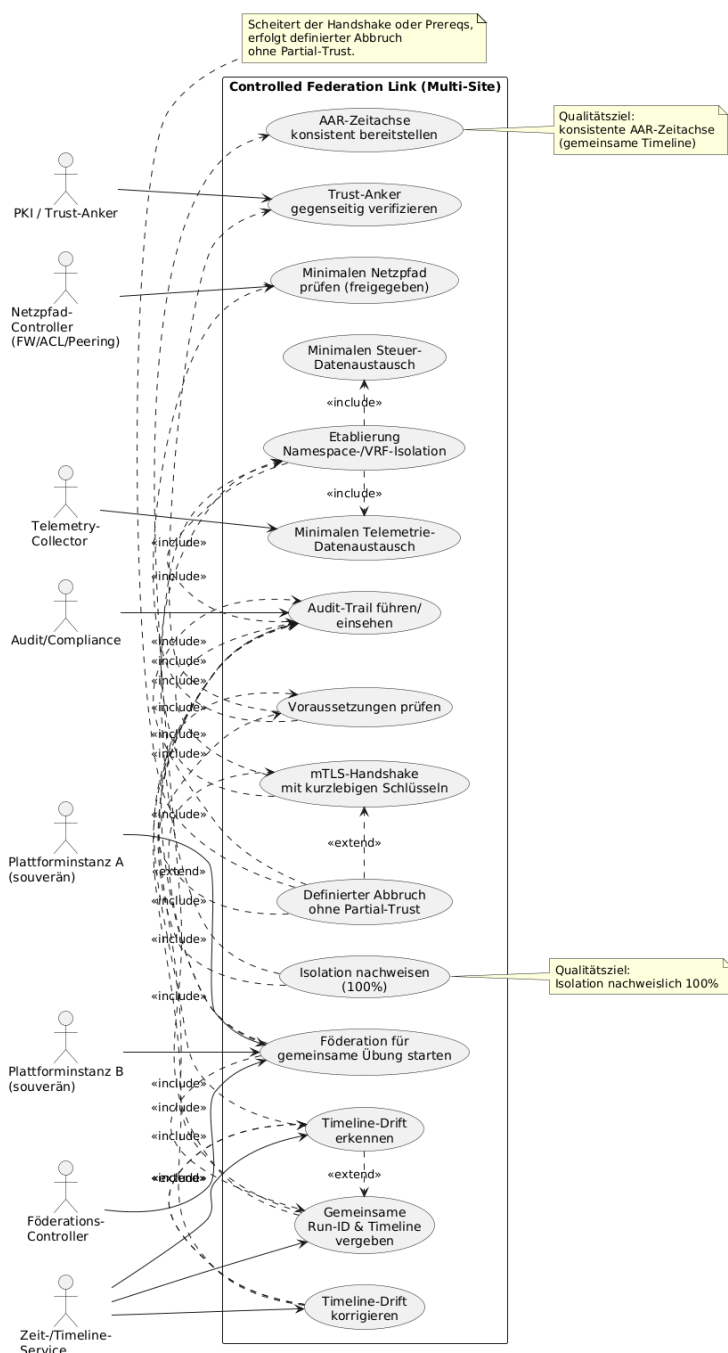


ABBILDUNG 9 FÖDERIERTE ÜBUNG KOPPELN

UC-06 – Realgerät anbinden (Hardware-in-the-Loop)

Ein reales Gerät wird über einen Adapter/Guard in ein Szenario integriert, nachdem ein Testpfad positiv verifiziert wurde. Policies (ein-/ausgehende Protokolle, Ratenbegrenzung) werden vor der Aktivierung festgelegt; jedes von Realquellen stammende Ereignis ist explizit zu markieren. Bei Policy-Verstößen wird die Verbindung sofort getrennt und alarmiert; bei unzulässiger Latenz wird auf Emulation zurückgegriffen. Erfolgskriterium ist vollständige Einhaltung der definierten Guards

und die eindeutige Kennzeichnung von Realereignissen. Damit stärkt der Use-Case die Anforderungen an Sicherheit, Beobachtbarkeit und Testbarkeit bei gleichzeitiger Wahrung der Übungsisolation.

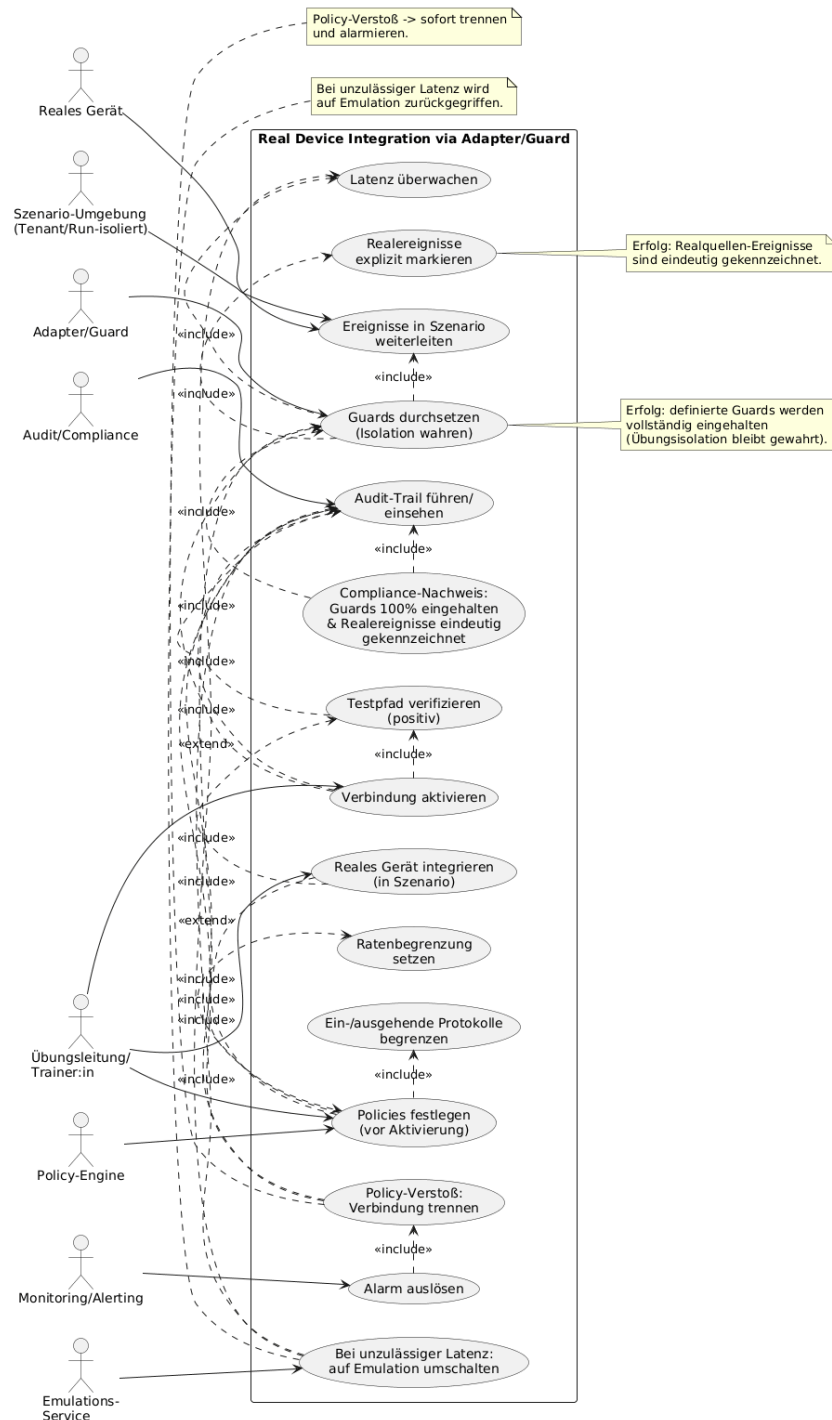


ABBILDUNG 10 REALGERÄT ANBINDEN

UC-07 – Observability & Triage

Trainer:innen und Beobachter:innen erhalten ein konsolidiertes Lagebild in Echtzeit. Die Interaktion umfasst das Setzen von Run-Filtern, die Korrelation von Ereignissen, Flows und Logs sowie Drill-downs mit selektivem Export. Grundlage bildet eine synchronisierte lokale Zeitbasis; Telemetrie ist konsequent Run-ID-gebunden. Unklare Korrelationen triggern Zeitbasisprüfungen,

Datenlücken werden als Importdefizite gekennzeichnet. Zielwerte sind $\geq 95\%$ zeitkorrelierte Events und Abfragezeiten < 2 s. Der Use-Case sichert die didaktische Steuerung und forensische Auswertbarkeit ab und verankert technische Anforderungen an MELT-Erfassung, Indizierung und Zugriff.

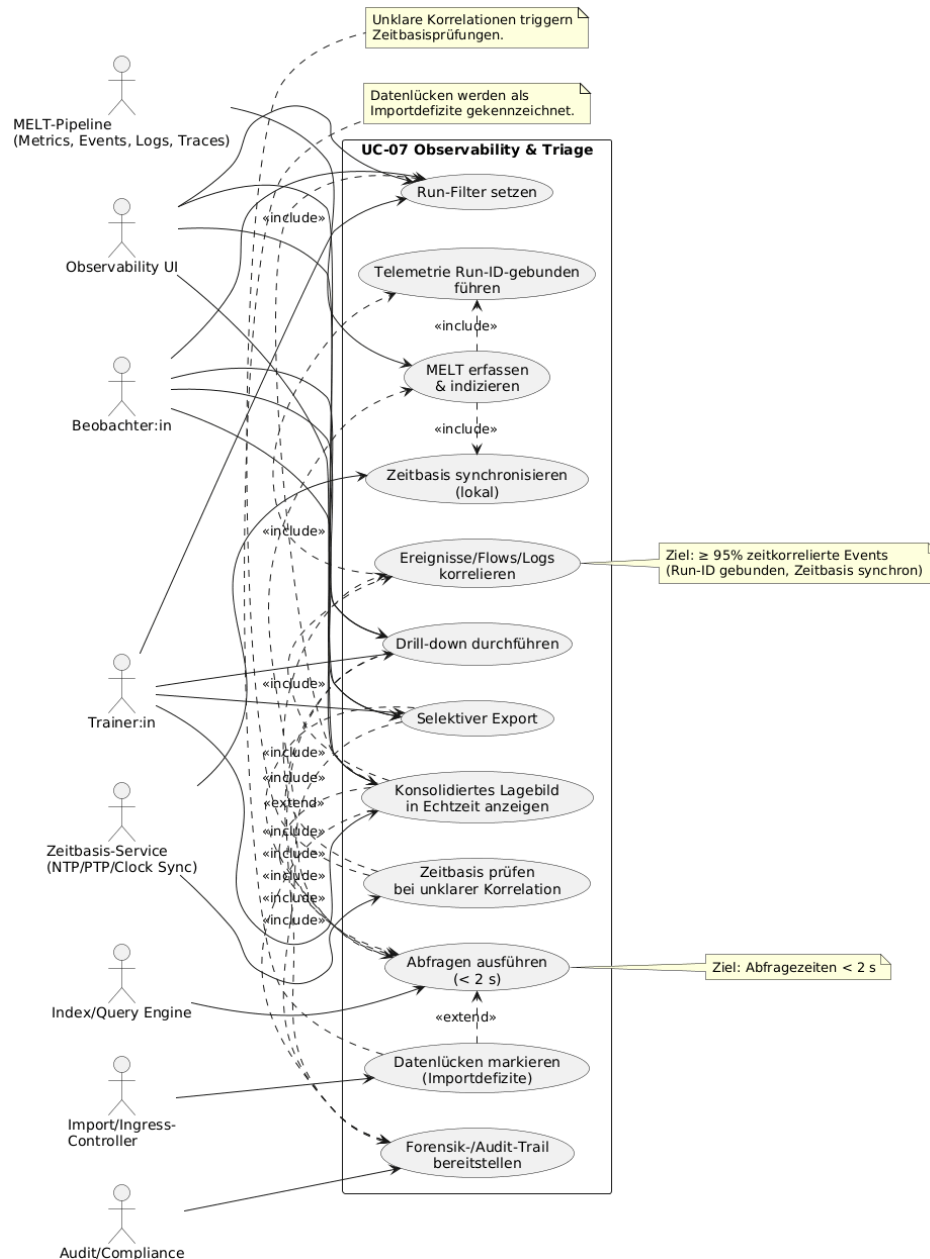


ABBILDUNG 11 OBSERVABILITY & TRIAGE

UC-08 – AAR erzeugen & exportieren

Nach Abschluss eines Runs aggregiert der AAR-Dienst Timeline, Artefakte, Scoring- und KPI-Daten zu einem signierten Exportpaket. Die Integrität wird über Hash/Signatur nachgewiesen; ein optionaler Anonymisierungsmodus minimiert personenbezogene Daten. Fehlen Teilinformationen, wird ein teilweiser Export mit Kennzeichnung ermöglicht; Signaturfehler führen zu deterministischem Abbruch mit Alarmierung. Maßgeblich ist ein deterministisches Replay kritischer Ereignisse sowie eine gültige Signatur/Prüfsumme. Der Use-Case adressiert

Nachvollziehbarkeit, Datenschutz und Integrität und schafft die Evidenzgrundlage für Abnahme und Forschungsauswertung.

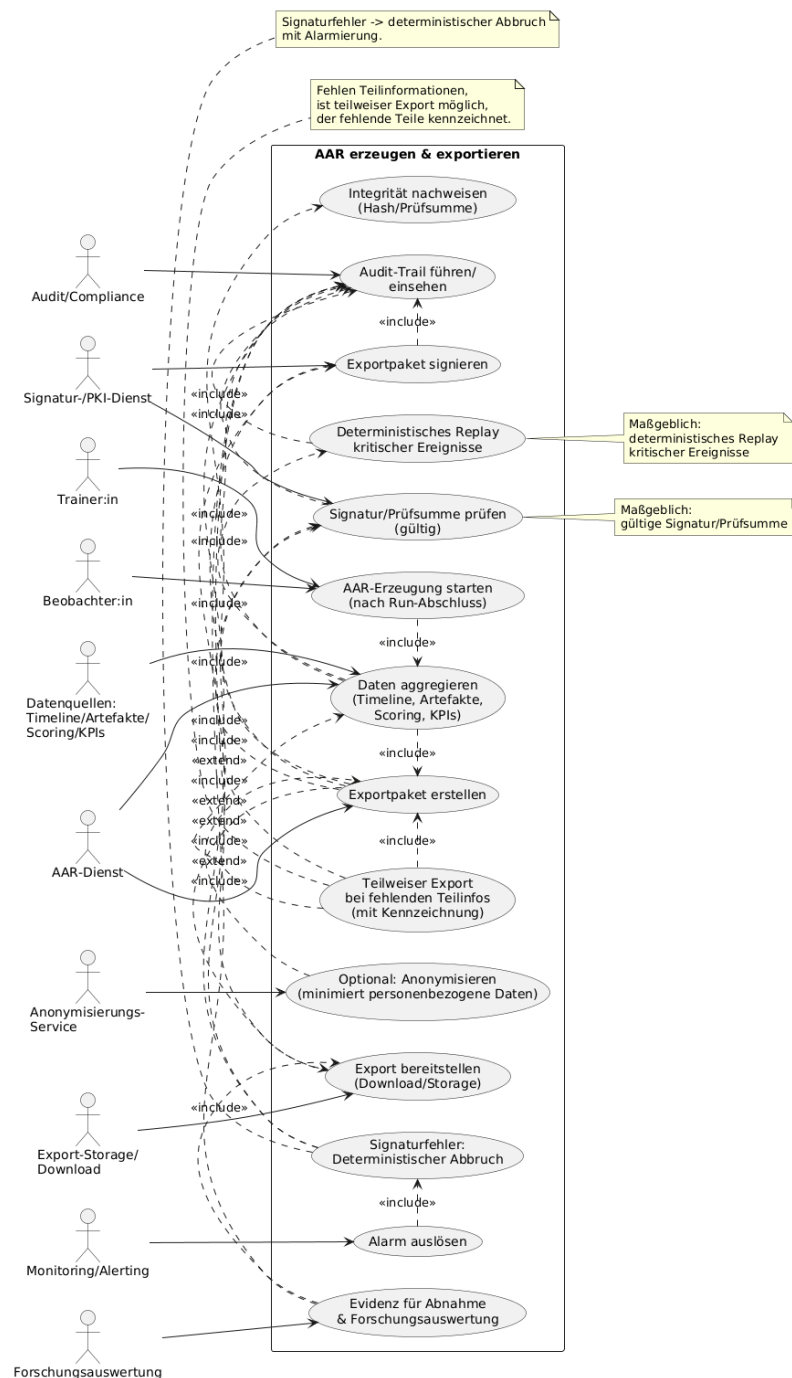


ABBILDUNG 12 AAR ERZEUGEN & EXPORTIEREN

UC-09 – Artefakt-Supply offline

Artefakte (Images, Charts, Pakete) werden aus lokalen Spiegeln importiert, gegen Signatur und SBOM geprüft und über ein Staging-Verfahren in die Produktion überführt. Ungültige Signaturen werden abgelehnt und alarmiert; SBOM-Abweichungen führen zur Quarantäne. Zielgrößen sind eine 100 %-Signaturprüfung und eine Ablehnungszeit < 2 s. Der Use-Case implementiert Lieferkettensicherheit unter Air-Gap-Bedingungen und stützt die Wartbarkeit durch kontrollierte Promotionspfade und revisionssichere Freigabeprotokolle.

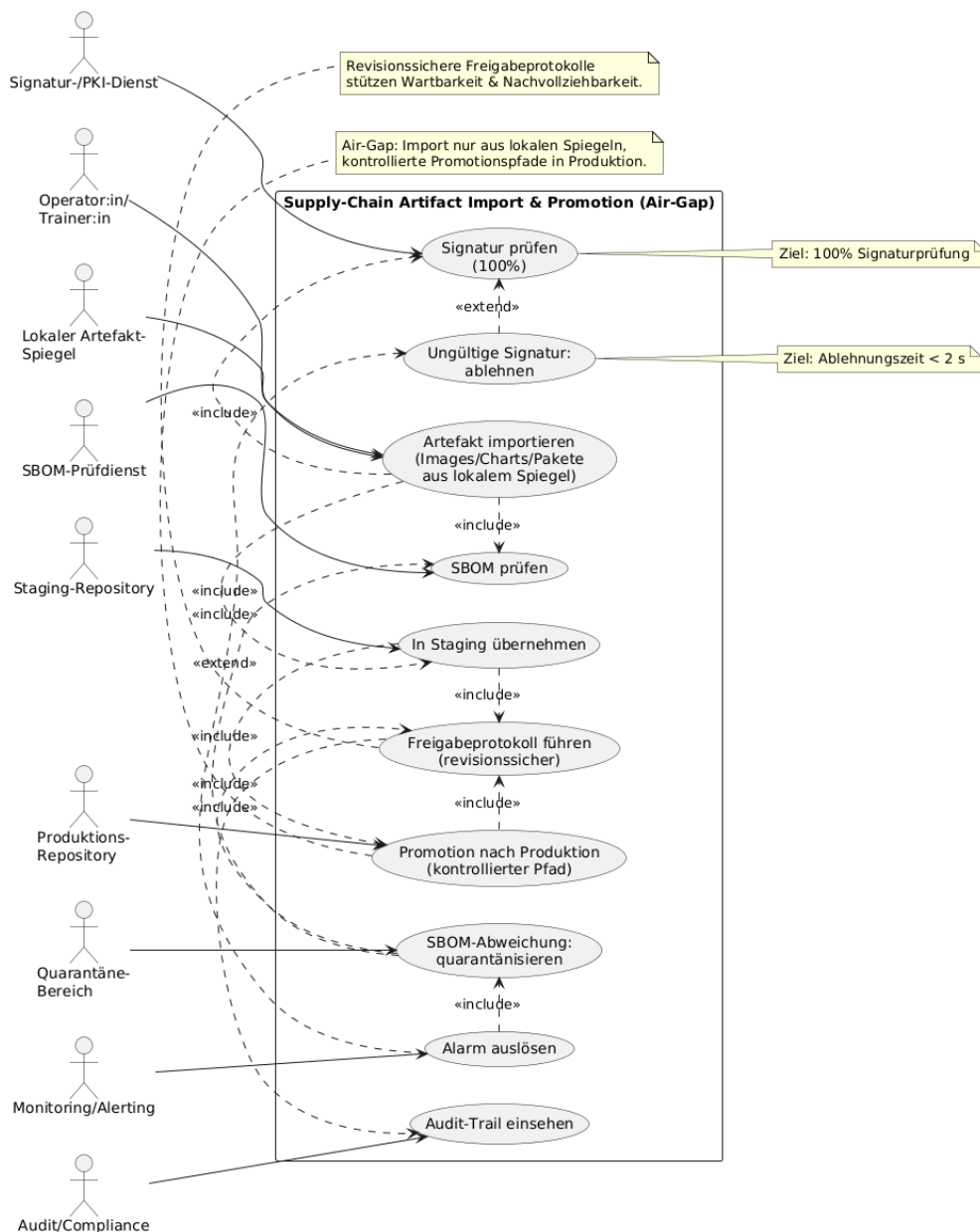


ABBILDUNG 13 ARTEFAKT-SUPPLY OFFLINE

UC-10 – Reset/Recovery/DR

Bei Störungen, Fehlbedienungen oder geplanten Übungen zur Notfallvorsorge wird ein Run auf einen „Known-Good-State“ zurückgesetzt, betroffene Dienste werden neu gestartet oder per Failover ersetzt und die Observability-Datenbank wiederhergestellt. Scheitert ein Reset, wird auf einen zweiten Snapshot-Stand gewechselt; ist kein Failover möglich, erfolgt eine geordnete Degradation mit Read-Only-AAR-Fähigkeit. Zielwerte sind ein Lab-Reset < 60 s und eine Wiederherstellung der Observability < 15 min. Der Use-Case konkretisiert Verfügbarkeits-, Resilienz- und Operabilitätsziele und stellt die Steuerbarkeit des Trainingsbetriebs auch unter Fehlerbedingungen sicher.

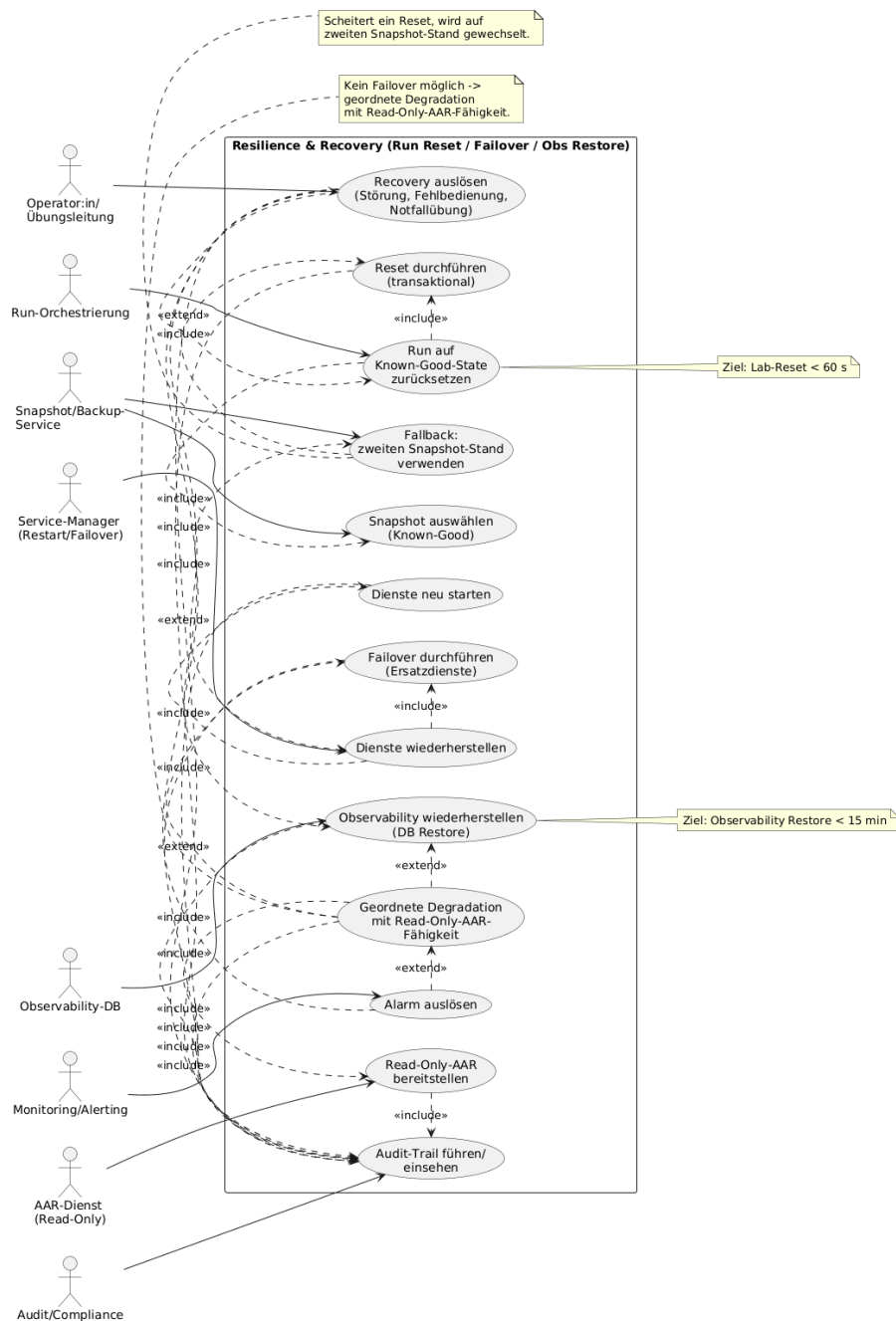


ABBILDUNG 14 RESET/RECOVERY/DR

Diese Use-Cases bilden eine in sich konsistente Kette vom modellierten Szenario (UC-01) über die reproduzierbare Bereitstellung (UC-02), die kontrollierte Durchführung (UC-03/-04/-05/-06), die Beobachtung und Bewertung (UC-07/-08) bis zur Artefaktversorgung und Störungsbewältigung (UC-09/-10). Jede Instanz enthält definierte Vorbedingungen, deterministische Abläufe, explizite Fehlerpfade und messbare Zielgrößen, wodurch Anforderungen, Architekturbausteine und Testfälle deckungsgleich verknüpft werden.

4.5 Referenzarchitektur A – VM-zentriert & HLA/DIS-föderiert

Die Referenzarchitektur A adressiert den Aufbau einer Trainingsplattform unter Bedingungen maximaler Kontrolle und Abschottung. Ausgangspunkt ist ein Virtualisierungs-First-Ansatz: Rechen-, Speicher- und Netzressourcen werden primär über VM-Cluster bereitgestellt; Container kommen—wo fachlich sinnvoll—gekapselt innerhalb von VMs zum Einsatz. Diese Entscheidung reduziert externe Abhängigkeiten, erhöht die Deterministik von Bereitstellung und Laufzeit und ermöglicht Snapshot-/Clone-basierte Betriebsprozesse, die für reproduzierbare Übungen und After-Action-Analysen zentral sind. Die Netzarchitektur folgt einem stabilen Segmentierungsmodell (z. B. VLAN/VRF und strikt getrennte Zonen für Management, Übung, Föderation, Observability), das Mandantentrennung, Least-Privilege-Durchsetzung und prüfbare Isolationsgarantien unterstützt—auch bei parallelen Runden und föderierten Szenarien.

Für die Kopplung über Standort- und Organisationsgrenzen hinweg setzt die Architektur auf bewährte Simulations- und Interoperabilitätsstandards: HLA/IEEE 1516 als föderatives Rahmenwerk mit formalen Objekt-/Interaktionsmodellen (FOM/SOM) und DIS/IEEE 1278 als leichtgewichtige Schnittstelle insbesondere für Live-Netzgeräte oder Gateways. Diese Standards bieten klare Semantik, wohldefinierte Schnittstellen und breite Werkzeugunterstützung; zugleich erlauben sie eine strikte Datenminimierung (nur der für die Übung notwendige Sichten-Austausch) und lokale Souveränität der beteiligten Sites. Föderationsverbindungen werden zeitlich begrenzt, zweckgebunden und kryptografisch (mTLS, kurzlebige Schlüssel) abgesichert, sodass die Air-Gap-Prämisse gewahrt bleibt.

Die Variante ist auf streng gekapselte, hochkontrollierte Umgebungen ausgelegt—etwa militärische Ausbildungssettings mit Offline-Betrieb als Grundannahme. Alle betriebskritischen Abhängigkeiten (Artefaktversorgung, Identität, Zeitbasis) werden lokal gespiegelt und mit Signaturen/SBOMs verifiziert; Szenarien, Policies und IaC-Definitionen sind Everything-as-Code und damit versionierbar, signier- und auditierbar. Der resultierende Determinismus in Provisionierung (Golden Images, Plan/Apply/Destroy), Laufzeitsteuerung (Start/Pause/Reset/Eskalation) und Beobachtbarkeit (Run-ID-gebundene MELT-Daten) bildet die Grundlage für objektive Bewertung und forensisch belastbare After-Action-Reviews.

Die Architektur priorisiert die Qualitätsattribute Sicherheit, Isolation, Reproduzierbarkeit und Nachweisbarkeit vor maximaler Elastizität. Gegenüber cloud-nativen Ansätzen sind Agilität und horizontale Skalierbarkeit bewusst nachgeordnet; Komplexität wird zugunsten robuster Kontrollmechanismen reduziert. Container-Workloads werden dort eingesetzt, wo sie didaktischen oder operativen Mehrwert stiften, jedoch ohne die VM-basierte Kontroll- und Härtehülle aufzubrechen. In Summe entsteht ein Plattformprofil, das SOC/NOC-Trainings, Cyber-Range-Szenarien sowie Hands-on-Labs unter strengem Governance-Regime zuverlässig trägt, förderierbar ist und Air-Gap-Evidenz methodisch erbringt.

4.5.1 Übersicht & Bausteine

Die Referenzarchitektur A priorisiert eine deterministische, air-gap-fähige Bereitstellung und Steuerung von Trainingsumgebungen. Grundlage ist ein Vier-Schichten-Modell, das Verantwortlichkeiten und Schnittstellen klar trennt und dadurch Wiederholbarkeit, Isolation und Prüfbarkeit erhöht. Auf der obersten Schicht „Management & Orchestrierung“ werden Szenarien als Code erfasst, syntaktisch/semantisch geprüft und über die Orchestrierung im gesamten Run-Lebenszyklus gesteuert; hierzu zählen die Ereignisinjektion, die rollenbasierte Zugriffskontrolle über einen lokalen Identitätsdienst (IdP/PKI), die gesicherte Bereitstellung aus Artefaktspiegeln sowie die Erstellung von After-Action-Reports (AAR). Die Schicht der „Simulations-/Übungs-Dienste“ stellt generische Mechanismen zur Verfügung, um Protokoll- und Verkehrsmuster zu erzeugen und Netzcharakteristika wie Latenz, Jitter und Paketverlust gezielt zu emulieren. Optional

werden Adapter für OT-Protokolle und Hardware-in-the-Loop unter strikten Guards eingebunden, um reale Geräte kontrolliert und nachvollziehbar zu beteiligen. Darauf aufbauend bieten „Trainings-Applikationen“ die didaktischen Frontends: Hands-on-Portale mit automatischem Scoring (z. B. Flag-Abnahme), Lernpfade mit geführten Hinweisen sowie Werkzeuge für Blue-, Red- und Purple-Team-Abläufe. Die Basisschicht „Infrastruktur (Compute/Storage/Netz)“ stellt mit gehärteten VM-Clustern, zugehörigen Storage-Pools und VRF/VLAN-segmentierten Netzen die technische Tragekonstruktion; dedizierte Föderations-VRFs entkoppeln Inter-Site-Verbindungen von den Übungssegmenten.

Die Kernkomponenten dieser Variante sind auf Offline-Betrieb und Nachweisbarkeit ausgelegt. VM-Cluster (Hypervisor) mit Snapshot-/Clone-Funktionen ermöglichen reproduzierbare Zustandsübergänge und kurze Wiederanlaufzeiten. Ein Artefakt-Repository für Images/OVAs erzwingt Signatur- und SBOM-Prüfungen, während ein lokaler Git-Mirror den Szenario- und Infrastruktur-Code (inklusive ADRs) mit signierten Tags/Merges verwaltet. Das IaC-Tooling—typischerweise Terraform/Ansible/Packer—deckt Plan/Apply/Destroy sowie deterministische Rebuilds ab; damit werden Golden Images konsistent erzeugt und gepflegt. Eine offline-fähige PKI/CA unterstützt Schlüssel-Lebenszyklen und Offline-CRLs, einschließlich kurzlebiger Föderationszertifikate. Der Observability-Stack erfasst Metriken, Events, Logs und Traces (MELT) run-gebunden und zeitlich konsistent; eine lokale Zeitquelle (NTP/GPS) stellt die deterministische Stempelung sicher. Ein streng konfigurierter Jump-Host dient als kontrollierter Einstiegspunkt mit lückenloser Protokollierung und definierten Break-Glass-Prozeduren. Zusammengekommen stützen diese Bausteine die geforderte Reproduzierbarkeit, Isolierbarkeit und Auditierbarkeit im air-gapped Betrieb.

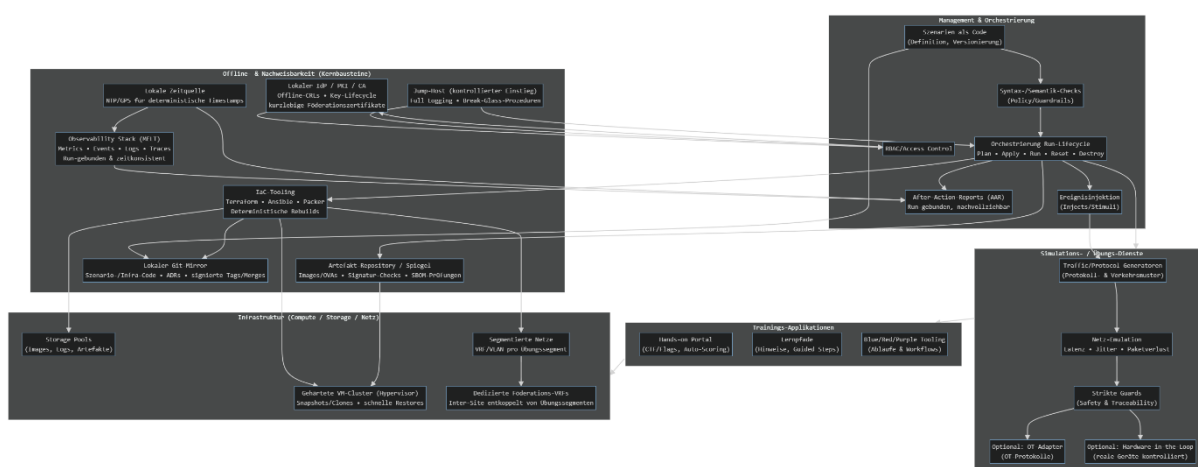


ABBILDUNG 15 ARCHITEKTUR A ÜBERSICHT DER BAUSTEINE

4.5.2 Technologie-Stack und Plattformkomponenten

Hier wird für die Referenzarchitektur ein Technologie-Stack beschrieben. Ziel ist es, die im vorhergehenden Abschnitt beschriebenen Bausteine und Sichten mit konkreten Technologie-Kategorien zu hinterlegen und damit eine konsistente, umsetzbare Plattformkonfiguration zu skizzieren. Es handelt sich ausdrücklich nicht um eine verbindliche Produktauswahl, sondern um ein Technologie-Profil, das als Referenz für nachgelagerte Beschaffungs- und Detaildesign-Entscheidungen dient.

Der Technologie-Stack ist so ausgelegt, dass er folgende, für Referenzarchitektur charakteristische Ziele unterstützt:

- Betrieb auf einer VM-zentrierten Infrastruktur mit klar getrennten Clustern und Zonen,

- deterministische Bereitstellung und Wiederherstellung von Zuständen (Snapshots, Clones),
- schwerpunktmäßig HLA/DIS-basierte Föderation von Simulationen und Umgebungen,
- Betrieb in unterschiedlich stark isolierten Umgebungen (bis hin zu weitgehend vom Internet entkoppelten Setups),
- durchgängige „Everything-as-Code“-Ausrichtung für Infrastruktur, Konfiguration und Sicherheitsrichtlinien.

Der folgende Überblick (Tabelle 6) fasst die zentralen Technologie-Kategorien zusammen und ordnet ihnen beispielhafte Komponenten zu.

TABELLE 6 TECHNOLOGIE-STACK REFERENZARCHITEKTUR (VM-ZENTRIERT)

Kategorie	Technologie-Profil	Rolle in Referenzarchitektur	Besondere Aspekte in RA
Virtualisierung / Hypervisor	KVM-basierte Clusterplattform, klassische Enterprise-Hypervisor, gehärtete Host-OS-Images	Bereitstellung der VM-Cluster, Isolation der Szenarien, Snapshots und Clones	Fokus auf deterministische Snapshots, konsistente Golden Images, getrennte Cluster je Sicherheits-/Lastprofil
Infrastruktur-Provisionierung & IaC	Terraform für Netzwerk/Cluster, Ansible für OS-/Service-Konfiguration, Image-Build-Werkzeuge (z. B. Packer)	Umsetzung von „Infrastructure-as-Code“ für Hosts, Netze und zentrale Services	Vollständig deklarative Beschreibung der Infrastruktur; Wiederaufbaufähigkeit auch in isolierten Netzen
Artefakt- und Imagebereitstellung	Lokales OVA-/Image-Repository, Objekt-Storage für Installationspakete und Konfigurationsartefakte	Versorgung der Plattform mit VM-Images, Paketen, Konfigurationen und Templates	Signierte Artefakte, Versionierung und Nachvollziehbarkeit von Änderungen, WORM-Speicherklassen für freigegebene Basisimages
Simulations- und Föderationsstack	HLA-RTI, DIS-Gateway, ggf. Netzemulationskomponenten (z. B. traffic shaping auf Basis systemnaher Tools)	Kopplung der einzelnen Simulationen und Umgebungen gemäß Föderationskonzept	Standardisierte Schnittstellen (HLA/DIS), definierte FOM/SOM, konfigurierbare

			Export-/Import-Sichten je Szenario
Plattform- und Laufzeitservices	VM-basierte Middleware- und Anwendungs-Stacks (z. B. Web-/Anwendungsserver, Messaging, Datenbanken)	Bereitstellung von Plattformdiensten für Orchestrierung, Steuerung und Auswertung	Trennung von „Plattform-VMs“ und „Szenario-/Simulations-VMs“; standardisierte Basiskonfigurationen
Observability / MELT	Zentrale Zeitreihendatenbank, Log-Store, Tracing-Komponente, Metrik-/Log-Forwarder auf den VMs	Sammlung und Auswertung von Metriken, Events, Logs und Traces (MELT)	Lauf-ID-bezogene Telemetrie, Export in AAR-Pakete, Betrieb in Netzen mit eingeschränkter Konnektivität
Identity & Access Management / PKI	Lokale PKI/CA, Identity Provider mit Rollen- und Gruppenverwaltung, Offline-verteilte Vertrauensanker	Authentisierung und Autorisierung von Nutzenden, Diensten und Administrationszugängen	Kurzlebige Zertifikate, abgestufte Rollenmodelle (z. B. Szenario-Owner, Operator, Auditor), Offline-Gültigkeitsprüfung
Secrets- und Schlüsselverwaltung	Zentraler Secrets-Tresor, Integrationen in Konfigurations- und Deployment-Werkzeuge	Sichere Ablage und Verteilung von Zugangsdaten, Schlüsseln und Tokens	Keine Klartext-Speicherung in Repositories oder State-Files; Vier-Augen-Prinzip für besonders kritische Geheimnisse
Sicherheits- und Netzrichtlinien	Zonen- und Segmentierungsregeln, Firewall-Konfigurationen, Härtingsrichtlinien und Baselines als Code	Durchsetzung der Sicherheitsarchitektur auf Netz- und Systemebene	Abbildung des Zonenmodells der Plattform in Firewalls und Hypervisor-Konfigurationen; automatisierte Compliance-Prüfungen
Management- und Betriebswerkzeuge	Zentralisierte Management-Konsole für Cluster und VMs, Konfigurations- und Patch-Management,	Unterstützen der Betriebsprozesse (Provisionierung,	Unterstützung wiederholbarer Betriebsabläufe, definierte Runbooks für

	Backup-/Restore-Lösungen	Patchen, Backup, Wiederherstellung)	typische Szenarien und Störungsfälle

Virtualisierungs- und Infrastrukturschicht

Die Virtualisierungs- und Infrastrukturschicht bildet das Fundament der Referenzarchitektur A. Ein konsistenter Hypervisor-Stack und gehärtete Host-Betriebssysteme stellen sicher, dass die verschiedenen Cluster (z. B. nach Sicherheitsniveau oder Systemrolle getrennt) zuverlässig und reproduzierbar betrieben werden können. VM-Snapshots und Clones werden systematisch genutzt, um definierte Ausgangszustände für Trainingsläufe herzustellen und diese bei Bedarf wiederherzustellen. Die hierfür notwendigen Konfigurationen (Netzsegmente, Speicherpools, Zugriffsrechte) werden vollständig als Code beschrieben.

Konfigurations- und Artefaktmanagement

Infrastrukturbeschreibung und Systemkonfiguration werden durchgängig in Form von IaC und Configuration-as-Code abgebildet. Terraform (oder ein vergleichbares Werkzeug) beschreibt Netze, Cluster und zentrale Platforddienste, während zustandsorientierte Werkzeuge (z. B. Ansible) die Betriebssystem- und Applikationskonfiguration der VMs übernehmen. Golden Images für wiederkehrende Rollen (z. B. „Simulationsknoten“, „Orchestrierungs-VM“, „Auswertungs-VM“) werden automatisiert erstellt, versioniert und in einem Image-Repository vorgehalten. Ein lokales Artefakt- und Objekt-Storage stellt sicher, dass alle für die Plattform notwendigen Pakete und Konfigurationen auch in stark eingeschränkt angebundenen Umgebungen zur Verfügung stehen.

Simulations- und Föderationsstack

Der Simulations- und Föderationsstack implementiert die in Referenzarchitektur A vorgesehenen HLA- und DIS-basierten Kopplungen. Ein HLA-RTI stellt den Kern der Föderation bereit, während Gateways/Bridges zu DIS und – falls erforderlich – zu weiteren Protokollen die Einbindung existierender Simulatoren und Testumgebungen ermöglichen. Die Festlegung und Versionierung von FOM/SOM, die Konfiguration zulässiger Export-/Import-Sichten sowie die Abbildung von Szenario-spezifischen Parametern erfolgen ebenfalls deklarativ und nachvollziehbar. Ergänzend können Netz-Emulationskomponenten eingesetzt werden, um definierte Netzbedingungen (Latenzen, Paketverlust, Bandbreitenbegrenzung) für Trainingszwecke reproduzierbar herzustellen.

Betriebs-, Sicherheits- und Observability-Funktionen

Die Plattform stellt zentrale Dienste für Observability (Metriken, Events, Logs, Traces), Identitäts- und Zugriffsverwaltung sowie Secrets-Mnagement bereit. Die Telemetrie-Infrastruktur ist so ausgelegt, dass Lauf-spezifische Daten mitgeführt und in AAR-Paketen ausgewertet werden können. Ein lokaler Identity Provider und eine interne PKI ermöglichen die Umsetzung eines fein granularen Rollen- und Rechtekonzepts sowie die Nutzung von Zertifikaten für Maschinen- und Dienstkommunikation. Sicherheits- und Netzrichtlinien (z. B. Segmentierung, Härtung, Protokollierung) werden als Code verwaltet und automatisiert auf die relevanten Komponenten angewendet. Ergänzende Management- und Betriebswerkzeuge unterstützen typische Betriebsprozesse wie die initiale Provisionierung, das Einspielen von Updates, Backup/Restore und die Wiederherstellung kompletter Szenarien.

Der hier skizzierte Technologie-Stack definiert damit ein konsistentes, VM-zentriertes Plattformprofil für Referenzarchitektur A. Er dient sowohl als Grundlage für einen prototypischen Aufbau der Plattform als auch als Referenz für spätere Varianten und konkrete Produktauswahlentscheidungen.

4.5.3 Integrations- & Föderationskonzept

Das Integrations- und Föderationsdesign folgt dem Grundsatz der minimalen, standardbasierten Kopplung bei voller Wahrung lokaler Souveränität. Inter-Site-Kommunikation erfolgt ausschließlich über dedizierte Föderations-VRFs bzw. VPN-Strecken, die kryptografisch mittels mTLS und kurzlebigen Schlüsseln abgesichert sind. Für die semantische Interoperabilität werden bewährte Simulationsstandards eingesetzt: Die High Level Architecture (HLA, IEEE 1516) bildet mit formalisierten FOM/SOM-Artefakten den föderativen Rahmen; pro Übung werden nur wohldefinierte Objekt- und Interaktionssichten freigegeben, sodass Datenminimierung und Zweckbindung durchgesetzt werden. Ergänzend ermöglicht ein DIS-Gateway (IEEE 1278) die Anbindung von Live-Netzgeräten oder leichten Simulationsquellen; notwendige Mappings und Filter werden über Export-Policies geregelt, um eine strikte Trennung zwischen Übungs- und Föderationssichten zu bewahren.

Föderierte Übungen werden als Site-to-Site-Szenarien vorbereitet und erst nach einem kontrollierten Handshake aktiviert. Pre-Staging bzw. Pre-Positioning stellt sicher, dass alle benötigten Artefakte (Images, Konfigurationen, Schlüsselmaterial) air-gapped vorliegen; die aktive Föderationsstrecke dient anschließend nur dem austauschminimalen Steuer- und Telemetrievekehr. Die Partner synchronisieren eine gemeinsame Run-ID und eine konsistente Zeitbasis; verbleibende Zeitdrift wird innerhalb definierter Toleranzen akzeptiert und im AAR explizit gekennzeichnet. Für reale Systemanteile sieht die Architektur Proxies und Adapter mit Guards sowie Rate-Limits vor; sämtliche Ereignisse aus Realquellen werden eindeutig markiert, sodass im AAR und bei Replays die Herkunft transparent bleibt. Ein Traffic-Replayer ermöglicht zudem die deterministische Wiedereinspielung synthetischer oder aufgezeichneter Daten, wodurch Vergleichbarkeit über Runs und Sites hinweg erreicht wird, ohne die Prinzipien der strikten Isolation und Zweckbindung zu verletzen.

4.5.4 Deploy-/Infrastruktur-View

Nachfolgenden wird die Referenz-Topologie beschrieben und das Netzdesign der VM-zentrierten, HLA/DIS-föderierbaren Trainingsplattform. Ziel ist eine deterministische, air-gap-fähige Bereitstellung mit klaren Fehlerdomänen, reproduzierbaren Deployments (IaC) und belastbaren Isolationsgarantien. Die Darstellung ist variantenneutral und bindet die Qualitätsziele aus den Use-Cases (u. a. Orchestrierungs-Latenz < 5 s, Hands-on-Reset < 60 s, ≥ 10 parallele Runden, Observability-Query < 2 s) als Planungsgrößen ein.

4.5.4.1 Referenz-Topologien

Single-Site Lab: Die Basiskonfiguration zielt auf einen Standort mit einem VM-Cluster und logisch getrennten Zonen (Management, Übung/Tenant, Föderation, Observability). Der Cluster stellt Compute- und Storage-Ressourcen über Ressourcenpools bereit; Szenarien werden per IaC deterministisch bereitgestellt. Für jede Übungsrunde wird ein isolierter Namensraum (VRF) mit zugehörigen VLANs erzeugt; die Mandantentrennung erfolgt durch strikt definierte Richtlinien (deny-by-default) an den Zonenübergängen. Die Observability-Schicht nimmt MELT-Daten write-controlled entgegen; Management- und Orchestrierungsdienste sind in einer separaten, gehärteten Management-Zone konzentriert. Diese Topologie ist für Entwicklungs-, Abnahme- und Ausbildungsszenarien mit moderater Parallelität (Richtwert: ≥ 10 Runden) ausgelegt und minimiert die operative Komplexität bei gleichzeitig hohem Reproduktionsgrad (Snapshots/Clones).

Multi-Site: Mehrere Standorte betreiben je einen eigenständigen VM-Cluster mit identischer Zonenlogik. Föderationen werden ausschließlich über dedizierte Föderations-VRFs/VPNs etabliert, kryptografisch gesichert (mTLS, kurzlebige Schlüssel) und zweckgebunden/zeitlich begrenzt. Jede Site wahrt lokale Souveränität; ausgetauscht werden nur minimal notwendige



Steuer- und Telemetriesichten (HLA-FOM/SOM, DIS-Mapping). Eine gemeinsame Run-ID und eine konsistente Zeitbasis (lokale NTP/GPS-Quelle, Drift-Toleranzen) sichern die AAR-Reproduzierbarkeit. Die Fehlerdomäne ist pro Site klar abgegrenzt; Föderationspfade sind gesondert monitorbar und throttle-bar. Multi-Site-Aufbauten ermöglichen skalierte Übungen (z. B. verteilte Blue/Red-Teams) bei erhaltener Segmentierung pro Run/Tenant.

Deployed/Field: Für den Feldbetrieb wird ein kompakter Edge-Aufbau verwendet (z. B. 2–3 Hosts je Micro-Cluster, lokaler Artefakt-Mirror, offline-fähige PKI/CA, GPS-basierte Zeitquelle). Der Footprint ist reduziert, die Artefaktversorgung erfolgt über Pre-Staging (Images/Configs/Keys). Netzseitig werden die identischen Zonen bereitgestellt, jedoch mit engeren Bandbreiten-/Latenzbudgets und strikter Priorisierung (z. B. Steuer-/AAR-Verkehr vor Bulk-Telemetrie). Optional kann eine Store-and-Forward-Strategie für Telemetrie genutzt werden, um Air-Gap-Phasen zu überbrücken. Diese Topologie priorisiert Robustheit, deterministische Wiederanlaufpfade (Snapshots) und einfache Bedienbarkeit unter eingeschränkten Ressourcen.

4.5.4.2 Netzdesign

Zonen und Segmentierung: Die Netzarchitektur folgt einem konsistenten Zonenmodell: (i) Management-Zone, (ii) Übungs-/Tenant-Zonen (pro Run eigene VRF mit zugehörigen VLANs/Subnetzen; optional OT-Segmente), (iii) Föderations-Zone (Gateways/Guards, mTLS-Termini, Schlüssellebenszyklen), (iv) Observability-Zone (MELT-Ingest, Zeitserien/Logs/Traces; write-controlled). Die Trennung erfolgt primär über VRFs (Mandantentrennung auf L3) und VLANs (Feinseparierung auf L2). Jeder Run erhält eine eigene VRF-Instanz mit deterministisch zugewiesenen Netzen; Namensraum-Kollisionen werden durch reservierte Präfixräume und automatisierte Vergabe verhindert. Policies-as-Code definieren explizite Allow-Listen und erzwingen den Grundsatz „deny-by-default“ an allen Zonenübergängen.

Guards und Kontrollpunkte: Zonenübergänge sind durch Guards abgesichert, die mindestens Folgendes leisten: (a) mTLS-Terminationspunkte mit kurzlebigen Zertifikaten, (b) paket- und anwendungsnahe Filter (Export-/Import-Policies), (c) Rate-Limiting/Traffic-Shaping für föderierte oder HIL-Pfadsegmente, (d) lückenlose Protokollierung (unveränderliche Logs, Run-ID-Bezug). Für Hardware-in-the-Loop werden zusätzlich Positiv-/Negativ-Tests gefordert; Ereignisse aus Realquellen sind im Datenstrom eindeutig zu markieren. Die Observability-Zone akzeptiert ausschließlich write-Flows aus Übungs-/Föderationszonen und stellt Lesezugriffe nur aus Management-/Beobachterrollen bereit.

Adressierungs- und Routing-Prinzipien: Pro VRF werden feste Präfixe vergeben; Lab-/Szenario-Netze werden deterministisch aus einem Pool abgeleitet (z. B. /24-Slices je Rolle/Zone). Inter-VRF-Kommunikation ist standardmäßig unterbunden. Föderations-VRFs führen ausschließlich zu Gateway-Termini; Transit in Tenant-VRFs ist unzulässig. Für zeitkritische Pfade (Orchestrierungs-Kommandos, Scoring-Events) werden niedrige Latenzbudgets eingeplant; Bulk-Telemetrie kann über prioritätsniedrige Queues laufen. Optional kann eine Overlay-Kapselung (z. B. VXLAN innerhalb einer VRF) genutzt werden, wenn physische L2-Domänen stark fragmentiert sind; die Mandantentrennung verbleibt auf VRF-Ebene.

Cross-Domain-Optionen: Wenn Informationsübertragungen zwischen unterschiedlich klassifizierten Domänen erforderlich sind, kommen zugelassene Cross-Domain-Mechanismen zum Einsatz. Bevorzugt werden (i) unidirektionale Pfade (z. B. Export von AAR-Paketen) über datendiodenartige Verfahren oder kontrollierte Sneakernet-Prozesse mit Malware-Scanning, Signaturprüfung und Inventarisierung, sowie (ii) protokollbewusste Guards mit strengen Content-Filtern, Schema-Validierung und Protokoll-Konformitätsprüfungen. Solche Übertragungen sind zweckgebunden, zeitlich limitiert, vollständig protokolliert und in der RTM nachvollziehbar.

Live-Steuerpfade über Cross-Domain-Schranken sind zu vermeiden; falls technisch zwingend, ist ein gesondertes Sicherheitsgutachten mit expliziten Metriken erforderlich.

Messpunkte und Nachweisführung: An jedem Zonenübergang sind Messpunkte zu definieren: Latenz (P95), Paketverlust, Policy-Verletzungen (Blockrate), TLS-Handshakes (Fehlerraten), Telemetrie-Verzögerungen (Ingest-Lag). Für die Übungs-VRFs werden automatische Isolations-Checks gefahren (z.B. Reachability- und Netzpolices-Tests vor Start). Ein 24-h-Disconnect-Test validiert die Air-Gap-Tauglichkeit; währenddessen dürfen keine externen Abhängigkeiten auftreten. AAR-Pakete enthalten die relevanten Netz- und Zeitparameter, sodass Replays deterministisch möglich sind.

Betriebs- und Wiederherstellungsaspekte: Deployments sind ausschließlich IaC-basiert; Änderungen an Netzen/VRFs/VLANs erfolgen über versionierte Pipelines mit Vier-Augen-Freigabe. Golden Images und Snapshots sichern definierte Wiederherstellungspunkte; ein Run-Reset auf „Known-Good“ ist innerhalb der Zielzeit bereitzustellen (< 60 s für Hands-on-Labs). Für Multi-Site-Föderationen sind Fail-Open/Fail-Closed-Strategien explizit festzulegen (Regelfall: Fail-Closed bei Policy-/Zertifikatsfehlern). Backup/Restore der Konfigurationen (Netz- und VRF-Definitionen, Policies-as-Code) folgt den Zielwerten (RTO ≤ 2 h, RPO ≤ 15 min für Metadaten).

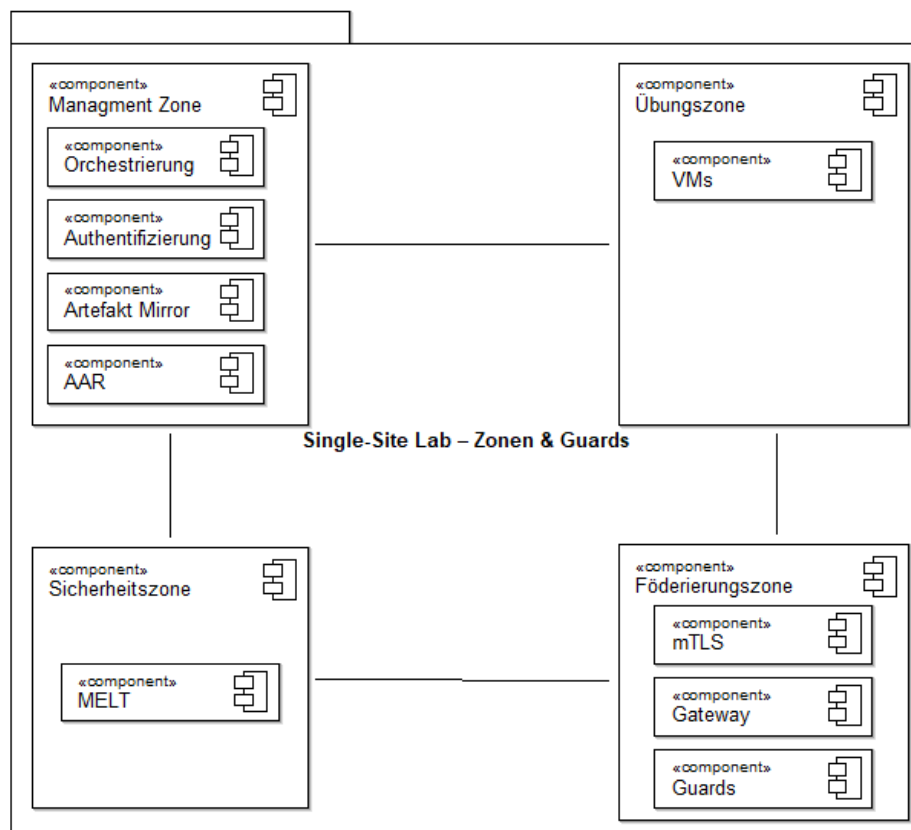


ABBILDUNG 16 SINGLE-SITE LAB – ZONEN & GUARDS

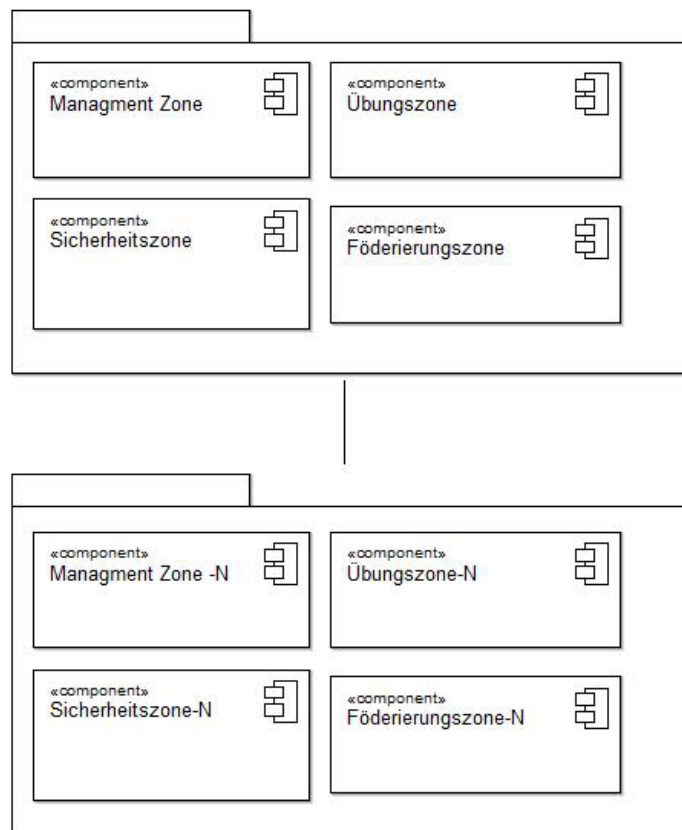


ABBILDUNG 17 MULTI-SITE – FÖDERATIONS-VRF/VPN ZWISCHEN SITES

4.5.5 IaC & Betriebsartefakte

Hier wird beschrieben wie die Gestaltung und den Betrieb der Infrastruktur-als-Code-Artefakte (IaC) sowie der zugehörigen Betriebsartefakte in der Referenzarchitektur A. Ziel ist ein deterministischer, auditierbarer und air-gap-fähiger Lebenszyklus, in dem Infrastruktur, Plattformdienste und Trainingsszenarien reproduzierbar entstehen, nachweislich gehärtet werden und ohne permanente Internetanbindung gepflegt werden können. Die Vorgehensweise bindet Governance-Vorgaben, Sicherheitsanforderungen und Qualitätsziele in eine konsistente Lieferkette ein, sodass Aufbau, Änderung und Wiederherstellung auf nachprüfaren, signierten Quellen beruhen.

Die IaC-Artefakte werden in drei logisch getrennten Repositories geführt, die unterschiedliche Verantwortlichkeiten und zeitliche Horizonte adressieren. Im Verzeichnis /infra/terraform sind Topologie, Ressourcen und Zonen definiert: Cluster- und Storage-Bereitstellung, VRF/VLAN-Strukturen, föderationsfähige Gateways und die für Szenarien benötigten Netzzräume. Die Terraform-Stacks sind modularisiert, strikt versioniert und werden mit aktivierter Drift-Detection betrieben; Zustände werden verschlüsselt, unveränderlich versioniert und in einem lokalen, vom Trainingsbetrieb getrennten Speicher gespiegelt. Im Verzeichnis /config/ansible liegen die System- und Applikationskonfigurationen, die Härtung von Hypervisoren und Gastsystemen, die Rollen- und Policy-Durchsetzung sowie die Konfiguration von Observability-Agenten, Scoring-Diensten und HIL-Adaptern. Ansible-Rollen sind idempotent, testbar und so strukturiert, dass Änderungen zuerst im Check-Modus validiert werden; sensiblere Parameter verbleiben außerhalb des Codes in einem offline betriebenen Geheimnis-Tresor. Das Verzeichnis /images/packer schließlich enthält die deterministischen Build-Spezifikationen für Golden Images im OVA-Format; es verankert feste

Paketquellen, unveränderliche Versionen und reproduzierbare Kompilationspfade, sodass identische Eingaben zu identischen Abbildungen führen.

Kern der Betriebsstrategie ist eine konsequente Golden-Image-Politik. Aus minimal gehärteten Basis-OVAs werden Rollenabbilder für Trainer-Konsolen, Blue-/Red-Team-Hosts, Observability-Ingest oder föderierte Gateways abgeleitet. In allen Fällen gilt: unnötige Dienste werden deaktiviert, kryptografische Basiseinstellungen sind konsistent und gegebenenfalls FIPS-tauglich, und nur ein kleiner Satz an First-Boot-Routinen bleibt für laufzeitnahe Feinparameter erhalten. Jedes Image trägt eine maschinenlesbare Stückliste (SBOM), eine Prüfsumme und eine Signatur des Build-Systems; darüber hinaus wird die Provenance der Erzeugung erfasst, also wer wann mit welchen Eingaben gebaut hat. Die Freigabe eines Images setzt erfolgreiche funktionale und sicherheitstechnische Prüfungen voraus, darunter Benchmarks zur Basis-Härtung, Offline-Malware-Scans, Start- und Dienstetests sowie Self-Checks zur Netzwerkisolation. Erst wenn mindestens drei Rebuilds in Folge sowohl artefakt- als auch hash-identisch ausfallen, wird ein Abbild in den Produktions-Mirror übernommen; der Mirror ist write-once-konfiguriert, sodass produktive Artefakte nur durch verifizierte Nachfolger ersetzt, nicht jedoch überschrieben werden.

Versionierung und Signaturen ziehen sich durch die gesamte Kette. Commits und Tags in den Repositories werden signiert, Merges erfolgen nach dem Vier-Augen-Prinzip, und Releases sind semantisch versioniert, mit klar ausgewiesenen Kompatibilitäten. Lockfiles der Konfigurationswerkzeuge sind ebenso signiert wie die Release-Notizen, die stets die relevanten Hashes, SBOM-Fingerprints und Verweise auf die Provenance enthalten. In den Ausführungs-Pipelines sind Signatur- und Hash-Prüfungen als blockierende Bedingungen implementiert; ein fehlgeschlagener Nachweis führt zum Abbruch der Ausführung. Widerrufte Schlüssel werden offline in Sperrlisten geführt, und betroffene Artefakte werden umgehend im Mirror gesperrt, sodass keine fehlerhafte oder kompromittierte Basis in Staging oder Produktion gelangen kann.

Der Offline-Patchprozess folgt einem streng gestuften Verfahren. Zunächst werden quellsseitige Spiegel außerhalb der Übungsnetze aktualisiert und als Snapshot eingefroren. Der Import neuer Pakete, Container-Charts oder OVAs erfolgt anschließend physisch in eine Quarantäne-Zone, in der Signaturen, Hashes und SBOMs geprüft und zusätzlich Offline-Scans ausgeführt werden. Erst danach wird in einer Staging-Umgebung auf Referenz-Hardware bereitgestellt: Die Terraform-Stacks werden geplant und angewendet, Ansible-Rollen im Check-Modus und anschließend in der Anwendung ausgeführt, und Packer-Images gegen die deklarierten Eigenschaften verifiziert. Funktionale Regressionstests prüfen Szenario-Provisionierung und Laufzeitsteuerung, Leistungsproben messen unter anderem die Bereitstellungszeit einer Standard-Range (Zielwert unter 30 Minuten) und die Orchestrierungs-Latenz bei Start, Pause und Ereignisinjektion (Zielwert unter fünf Sekunden im 95-Perzentil). Sicherheitsprüfungen kontrollieren die Einhaltung von Policies-as-Code, die korrekte Durchsetzung der Zonenisolation und die Abwesenheit unerlaubter Außenverbindungen, insbesondere im 24-Stunden-Disconnect-Test. Erst nach dokumentierter Abnahme und Signatur der Release-Artefakte erfolgt die Promotion in den Produktions-Mirror, der Trainingsbetrieb erhält die Änderungen in einem definierten Wartungsfenster und stets mit Rückrollmöglichkeit auf den zuletzt bekannten, signierten Stand.

Die IaC-Pipeline ist in Validierung, Planung, Test, Anwendung, Freigabe und Archivierung gegliedert, arbeitet vollständig offline mit lokalen Runnern und führt in jeder Stufe nachvollziehbare, deterministische Prüfungen durch. Format- und Schema-Validierungen stellen syntaktische Korrektheit sicher; Richtlinienprüfungen verwehren den Einsatz nicht genehmigter Ressourcen oder offener Ausgänge. In der Planungsphase erzeugt Terraform driftfreie Pläne, während Packer deterministische Builds liefert und Ansible zunächst im Check-Modus ohne Änderungen läuft. Testphasen decken Unit- und Molecule-Tests der Rollen, Infrastrukturtests zu Netzpfaden und Ports sowie Start- und Dienstesmoke-Tests ab. Die Anwendung in Staging ist mit Zeitbudgets versehen; bei Verstößen oder Fehlfunktionen erfolgt ein automatischer Rollback auf den zuletzt

bekannten, funktionsfähigen Zustand. Nach erfolgreichem Durchlauf werden die Artefakte signiert, die Release-Notizen aktualisiert und die Promotion freigegeben; sämtliche Zustände, Protokolle und Prüfberichte werden unveränderlich archiviert, um spätere After-Action-Analysen zu stützen.

Die Kopplung zu den Qualitätszielen der Plattform erfolgt nicht nur auf der Ebene der Tests, sondern auch im laufenden Betrieb. So werden die in den Use-Cases geforderten Kennzahlen – etwa die Bereitstellung einer Standard-Range unter einer halben Stunde, Reset-Zeiten von Hands-on-Labs unter einer Minute und Antwortzeiten auf Orchestrierungsbefehle unter fünf Sekunden – als Pipeline-Schranken, als Betriebsalarme und als Abnahmekriterien verankert. Für die Beobachtbarkeit gilt, dass die Ingest-Pfade der MELT-Daten vollständig und run-gebunden arbeiten und typische Abfragen auf den bereitgestellten Dashboards innerhalb von zwei Sekunden beantwortet werden. Die AAR-Pakete verknüpfen schließlich die verwendeten Artefakte über Versionen, Hashes und SBOM-Fingerabdrücke, sodass Replays kritischer Ereignisse deterministisch und überprüfbar sind.

Ein besonderes Augenmerk liegt auf Wiederherstellung und Re-Konstitution. Die Plattform muss im Worst-Case allein aus Code und signierten Artefakten neu aufgesetzt werden können. Dazu existieren Offsite-Kopien der Repositories, Terraform-Zustände und Mirrors in verschlüsselter, versionierter Form sowie Bare-Metal-Runbooks, die den Neuaufbau der Hypervisor-Ebene, die Grundkonfiguration des Netzes, die Rückführung der Terraform-Stacks und die erneute Anwendung der Ansible-Härtung beschreiben. Der Wiederanlauf priorisiert die Wiederherstellung der Zeitquelle und der PKI als Vertrauensanker, gefolgt von Observability-Ingest und Orchestrierung und erst danach den Übungsrollen. Für diese Vorfälle sind Zielwerte definiert: eine Wiederanlaufzeit zentraler Dienste von höchstens zwei Stunden und ein maximaler Datenverlust für Metadaten von fünfzehn Minuten. Jeder Drill wird protokolliert und als AAR mit Artefaktbezügen archiviert, sodass die Eignung der Verfahren periodisch nachgewiesen werden kann.

4.5.6 Sicherheit & Betrieb

Dieses Unterkapitel beschreibt die betrieblichen und sicherheitstechnischen Leitplanken der Referenzarchitektur A. Der Schwerpunkt liegt auf einem streng segmentierten Zonenmodell, systematischen Härtingsleitlinien für Hypervisor, Gäste und Betriebsprozesse, einem Backup/Restore-Regime mit klaren RTO/RPO-Zielen sowie einer Observability-Architektur für Monitoring und Logging. Alle Maßnahmen sind auf Air-Gap-Fähigkeit, Reproduzierbarkeit und Auditierbarkeit ausgelegt und schließen an die in 5.1–5.4 definierten Artefakte und Prozesse an.

4.5.6.1 Zonenmodell und Durchsetzungsprinzipien

Die Netz- und Sicherheitsarchitektur folgt einem konsistenten Zonenmodell mit Management-, Übungs-/Tenant-, Föderations- und Observability-Zone. Die Trennung erfolgt primär über VRFs (Mandantentrennung auf L3) und VLANs (Feinseparierung auf L2). Jede Übungsrunde erhält eine eigene VRF mit deterministisch zugewiesenen Präfixen; die Management-Zone ist physisch/logisch gesondert und exponiert ausschließlich gehärtete Orchestrierungs- und Katalog-APIs. Die Observability-Zone nimmt write-only Telemetrieflüsse auf (Metriken, Events, Logs, Traces/Flows) und gestattet nur autorisierten Rollen read-only Zugriff; Föderationspfade sind über eine dedizierte Föderations-VRF/VPN geführt.

Durchsetzung erfolgt über Guards an allen Zonenübergängen: (i) mTLS-Terminationspunkte mit kurzlebigen Zertifikaten, (ii) Policy-Filter (Export/Import, Protokoll-/Inhaltsvalidierung), (iii) Rate-Limiting/Traffic-Shaping auf föderierten und HIL-Pfadsegmenten, (iv) vollständige Protokollierung mit Run-ID-Bezug. Deny-by-default ist an allen Grenzen verpflichtend; Ausnahmen werden als Policies-as-Code versioniert und getestet. Für Hardware-in-the-Loop sind Positiv-/Negativtests vor Aktivierung, Ereignismarkierung „Realquelle“ und definierte Trennkriterien (Sofort-Disconnect bei

Policy-Verstoß) vorgelagert. Zeitkonsistenz ist durch eine lokale Zeitquelle (NTP/GPS) und disziplinierte Verteilung in alle Zonen sicherzustellen; Telemetrie wird konsequent run-gebunden erfasst.

4.5.6.2 Härtingsleitlinien (Plattform, Gäste, Prozesse)

Die Härtung orientiert sich an anerkannten Baselines, ist jedoch air-gap-tauglich operationalisiert und in Golden Images (5.4) verankert. Für den Hypervisor-Cluster gelten: minimale Installationsprofile, Secure/Measured Boot (soweit verfügbar), Signaturprüfung von Updates, Deaktivierung nicht benötigter Managementdienste, strikte Trennung von Management- und Storage/VM-Traffic, durchgängige AAA mit rollenbasierten Rechten (Least Privilege) und vollständige Sitzungsaufzeichnung an Bastion-Zugängen. Konfigurationsänderungen erfolgen ausschließlich über IaC-Pipelines mit Vier-Augen-Freigabe; interaktive Notfallzugriffe („Break-Glass“) sind protokollpflichtig und zeitlich begrenzt.

Für Gastsysteme/Applikationen gilt: Diensteminimierung, restriktive Kernel/Netz-Parameter, einheitliche Crypto-Policies, Härtung von SSH/WinRM, Protokollierung auf Host-Ebene mit Forwarding in die Observability-Zone (write-only), Disk-Verschlüsselung dort, wo Trägermedien die Zone verlassen können, und deterministische First-Boot-Hooks für Run-spezifische Minimalparameter. Secrets-Management erfolgt offline (versiegelter Tresor, rotierbare Bundles), niemals im Klartext in Repos oder States. Patch-Fenster sind gebündelt, werden über Quarantäne → Staging → Produktion abgewickelt und unterliegen Disconnect- und Regressionstests (kein Outbound außerhalb definierter Guards, 24-h-Nachweis).

Prozesshärtung umfasst: signierte Commits/Tags, verpflichtende Pipeline-Checks (Lint/Policy/Signature/SBOM), Change-Advisory für risikobehaftete Änderungen (Föderation, HIL, Netzwerkgrenzen), Pflicht-Rollbacks (Snapshots) und periodische Table-Top/Red-Team-Tests gegen Segmentierung, RBAC und Föderations-Guards. Alle Abnahmen erzeugen audit-feste Evidenz (Hashes, Signaturen, Testergebnisse), die in AAR-Paketen referenziert werden.

4.5.6.3 Backup/Restore (RTO/RPO) und Re-Konstitution

Das Sicherungskonzept trennt konfigurations-/codebasierte Artefakte (Repos, IaC-States, Policies, Golden-Image-Definitionen), Laufzeit-Artefakte (AAR-Pakete, Telemetrie, Logs) und Image-Spiegel (OVAs/Container). Backups sind verschlüsselt, signiert und mediengetrennt (WORM-Speicher bzw. offline rotierte Medien mit Inventarisierung). Empfohlen ist ein GFS-Schema mit täglichen inkrementellen und wöchentlichen Vollsicherungen für Metadaten/States sowie periodische Offline-Snapshots der Artefakt-Spiegel.

Zielwerte:

- RTO zentrale Management-/Orchestrierungsdienste ≤ 2 h (unter Annahme verfügbarer Referenz-Hardware),
- RPO Metadaten/States ≤ 15 min, AAR/Telemetrie entsprechend der Retentionspolitik (z. B. 12–24 Monate) mit differenzierter Priorisierung.

Wiederherstellungspfad (DR): Zunächst Zeitquelle und PKI/CA als Vertrauensanker, dann Observability-Ingest und Orchestrierung, anschließend Übungsrollen. Bare-Metal-Runbooks für Hypervisor-Neuaufbau, Netz-Grundkonfiguration, Einspielen von /infra/terraform und /config/ansible sowie Re-Aktion der Golden Images sind verpflichtend. DR-Drills werden mindestens halbjährlich durchgeführt; Nachweise (Dauer, Wiederanlaufpunkte, Abweichungen) fließen in AARs und ADRs ein. Medien-Kette (Chain of Custody) und Medien-Hygiene (Offline-Scan, Signaturprüfung vor Restore) sind dokumentationspflichtig.

4.5.6.4 Monitoring & Logging (Observability/MELT)

Die Observability-Architektur erfasst Metriken, Events, Logs, Traces/Flows (MELT) run-gebunden und zeitkonsistent. Ingest-Pfade sind write-controlled (keine Rückkanäle in Tenant-Zonen), und alle Datensätze tragen Run-ID und präzise Zeitstempel aus der lokalen Zeitquelle. Index-/Korrelationsdienste ermöglichen zeitnahe Triagen; als Betriebsziel gelten Query-Antwortzeiten < 2 s (P95) für definierte Standard-Sichten. Dashboards spiegeln die Qualitätsziele der Plattform (Provisionierungszeiten, Orchestrierungs-Latenzen, Reset-Dauern, Ressourcenquoten) und sind mit Alarmregeln (SLO-Verletzungen, Policy-Drifts, Telemetrie-Lag, Föderations-Handshake-Fehler) hinterlegt.

Log-Integrität wird durch verkettete Hashes, signierte Batches und unveränderliche Ablage (WORM/Append-only) gewährleistet; Exporte werden als signierte AAR-Anhänge bereitgestellt. Datenschutz ist über Datenminimierung (nur erforderliche Sichten), Rollen-basierte Leserechte und Anonymisierungs-/Pseudonymisierungsmodi im Export umzusetzen. Für föderierte Übungen werden Sichtschnitte explizit definiert (HLA FOM/SOM, DIS-Mappings) und im Ingest markiert; Timeline-Drift wird erkannt, toleriert im festgelegten Fenster und im AAR gekennzeichnet.

Betriebliche Routinen umfassen tägliche Gesundheitschecks (Zeitbasis, Ingest-Lags, Dropped Events), Kapazitätsprognosen (Storage/Index/Throughput) und Mutationstests der Alarmregeln. Messpunkte an Zonenübergängen (Latenz, Blockrate, TLS-Fehler) werden kontinuierlich erhoben; Abweichungen führen zu Policy-Revalidierung oder Traffic-Drosselung auf Föderations-/HIL-Pfaden. Alle Observability-Komponenten sind über IaC definiert; Änderungen unterliegen denselben Signatur-/Freigaberegeln wie Infrastruktur und Images.

4.5.7 Risiken

Die wesentlichen Risiken der Referenzarchitektur A werden nachfolgenden zusammengefasst. Der Fokus liegt auf einem VM-zentrierten, air-gap-fähigen Aufbau mit HLA/DIS-Föderation und optionaler HIL-Anbindung. Die Risiken werden domänenspezifisch beschrieben (Ursache/Wirkung), mit Indikatoren zur Früherkennung sowie mit konkreten Maßnahmen zur Risikobehandlung verknüpft. Ziel ist eine belastbare Grundlage für Architekturentscheidungen, Abnahme und den laufenden Betrieb.

4.5.7.1 Vorgehensweise und Bewertungsrahmen

Die Bewertung folgt einem pragmatischen, auditierbaren Rahmen, der Elemente aus FMEA/ISO-31000/ISO-27005 kombiniert:

- Risikobeschreibung (Bedrohung, Schwachstelle, betroffener Wert),
- Eintrittswahrscheinlichkeit und Auswirkung (je qualitativ: niedrig/mittel/hoch),
- Leitindikatoren/Detektionsmechanismen (Messgrößen, Alarmer, Tests),
- Behandlung (Vermeiden, Vermindern, Übertragen, Akzeptieren),
- Restrisiko und Nachweisführung (Test-/Auditartefakte, AAR-Referenzen).

Die hier aufgeführten Maßnahmen referenzieren die bereits definierten Mechanismen aus 5.1–5.5 (z. B. IaC-Pipelines, Golden-Image-Strategie, Zonen/Guards, Observability, DR-Runbooks).

4.5.7.2 Risikokatalog (Referenzarchitektur A)

Die Tabelle 7 fasst die wesentlichen Risiken der VM-zentrierten, HLA/DIS-förderierbaren Plattform zusammen. Pro Eintrag sind Ursache, Wirkung, Indikatoren, Maßnahmen und Restrisiko/Nachweise angegeben.

TABELLE 7 RISIKOKATALOG A

ID	Risiko (Kurzbezeichnung)	Ursache	Wirkung	Indikatoren	Maßnahmen/ Behandlung	Restrisiko & Nachweise
R-A1	Lieferkette/ Artefaktmanipulation (Supply Chain)	Kompromitierte Upstream-Artefakte, gestohlene Signatur- schlüssel, unvollständige SBOMs.	Integritätsverlust der Plattform/Übungs- umgebung.	Signatur-/Hash- Mismatch, SBOM- Diff- Alarme, erhöhte Ablehnungsrate in Quarantäne, ungewöhnliche Provenance.	Verpflichtende Signatur- und SBOM- Prüfung, Quarantäne- Import, Offline- AV/Static- Scan, Vier- Augen- Promotion, WORM- Mirrors, Schlüsselverwaltung mit Offline-CRLs und kurzlebigen Build-Keys.	Gering- mittel; Evidenz: Ablehnungsprotokolle, signierte Release- Notes, Provenance- Atteste.
R-A2	Konfigurations-/Image- Drift	Manuelle Änderungen, divergierende Rollens- OVAs, inkonsistente Hotfixes.	Verlust von Reproduzierbarkeit/Abnahmefähigkeit.	Terraform- Drift, Compliance- Abweichungen, Hash- Änderungen ohne Release.	Immutable Golden- Images, IaC- only-Changes, Drift- Detection, periodische Rebuilds, Molecule/Compliance- Tests.	Niedrig; Nachweis: identische Rebuilds (≥3×), leere terraformplan auf Referenz- Targets.
R-A3	Ressourcenengpässe/ vertikale Skalierung	VM- Zentrik, gleichzeitige Runden, Engpässe in Storage/CPU/Netz.	Erhöhte Latenzen, Zielverletzungen (z. B. Reset > 60 s).	Quota- Verletzungen, Orchestrierungs-Lags, Telemetrie- Backpressure.	Pre-Flight- Checks, Quotas, Kapazitätsplanung je Topologie, Lasttests, Scheduling- Regeln, geordnete Degradation.	Mittel; Nachweis: Kapazitätsberichte, SLO-Dashboards, Lasttest-AARs.
R-A4	Föderationskomplexität/ HLA-	Schema- Drift, inkompatible Sichten,	Inkonsistente Timeline/Telemetrie, Sicherheitslücke	Handshake-Fehler, Mapping-Warnungen	Strikte FOM/SOM- Governance, Schema-	Mittel; Nachweis: Föderati

ID	Risiko (Kurzbezeichnung)	Ursache	Wirkung	Indikatoren	Maßnahmen/ Behandlung	Restrisiko & Nachweise
	FOM/DIS-Mapping	fehlerhafte Namensräume.	en durch zu breite Exporte.	n, Timeline-Drift-Alarme.	Validierung, minimaler Sichten-Austausch, dedizierte Föderations-VRFs, mTLS kurzlebig, AAR-Kennzeichnung von Drift.	ons-Tests, Guard-Protokolle.
R-A5	HIL-Integration (Realgerät)	Unzureichende Isolation, fehlerhafte Adapter/Policies.	Unkontrollierte Flüsse, Seiteneffekte auf Übungsnetze.	Policy-Verstöße, Rate-Limit-Hits, unmarkierte „Realquelle“-Events.	Guards mit Positiv/Negativ-Tests, Rate-Limits, Ereignismarkierung, sofortiger Disconnect, Emulations-Fallback.	Mittel; Nachweis: Testprotokolle, Guard-Logs.
R-A6	Air-Gap-Erosion	Temporäre Links bleiben offen, versteckte Updater/Telefonate, Fehlkonfiguration.	Externe Abhängigkeiten, erweiterte Angriffsfläche.	Outbound-Versuche im 24-h-Disconnect-Test, DNS/TLS-Anomalien, egress-Firewall-Hits.	Harte egress-Policies, periodische Disconnect-Tests, Offline-Spiegel, Monitoring unerlaubter Verbindungen, Freigabeprozesse.	Niedrig-mittel; Nachweis: Testberichte, Firewall-Audits.
R-A7	Observability-Blindspots/Log-Integrität	Unvollständiger Ingest, Zeitdrift, manipulierte Logs.	Eingeschränkte Triage/Forensik, AAR nicht belastbar.	Ingest-Lag, Drop-Rate, Lücken in Run-ID-Korrelation, Hash-Ketten-Brüche.	Write-only Ingest, Run-ID-Pflicht, lokale Zeitquelle, verkettete Hashes, WORM-Speicher, SLO für Queries (<2 s).	Niedrig; Nachweis: Integritätsprotokolle, Sampling-Berichte.
R-A8	Identität/PKI offline	Ablaufende CRLs/Zertifikate, Schlüsselkompromittierung, fehlende OCSP-	AuthN/Z-Störungen, Vertrauensbruch.	Zertifikatswarnungen, fehlgeschlagene mTLS-Handshakes, Token-	CRL-Pflege offline, kurzlebige Zertifikate, Rotation, Dual-Control, Rollover-Drills.	Mittel; Nachweis: Key-Inventar, Rotationssprotokolle.

ID	Risiko (Kurzbezeichnung)	Ursache	Wirkung	Indikatoren	Maßnahmen/ Behandlung	Restrisiko & Nachweise
		Verfügbarkeit.		Ablauf-Spitzen.		
R-A9	Backup/Restore/DR-Versagen	Fehlerhafte/incomplete Sicherungen, verlorene Schlüssel, ungetestete Runbooks.	Verlängerte RTO/RPO, Datenverlust.	Fehlgeschlagene Restore-Tests, Prüfsummen-Fehler, veraltete Medien.	3-2-1 inkl. offline, GFS, verifizierte Checksummen/Signaturen, Restore-Drills, Chain-of-Custody.	Niedrig-mittel; Nachweis: Drill-AARs, Medieninventar.
R-A10	Fehlbedienung/Menschliche Faktoren	UI-Fehler, falscher Run-Kontext, irrtümliche Event-Injection.	Übungsabbrüche, falsche Bewertungen.	Anormale Abbruchraten, Undo/Reset-Zunahmen, Audit-Flags.	RBAC/Least-Privilege, Kontextanzeigen, Bestätigungen, Dry-Run, Schulungen/Runbooks, Vier-Augen-Prinzip.	Mittel; Nachweis: UI-Telemetrie, Schulungsnachweise.
R-A11	Lizenzierung/Compliance/Export	Offline-Lizenzen abgelaufen, OSS-Pflichten ignoriert, Exportkontrollen verletzt.	Rechtliche Risiken, Betriebsunterbrechungen.	Lizenz-Warnings, OSS-Scanner-Findings, Export-Policy-Alerts.	Lizenz-Spiegel/Entitlement-Checks offline, OSS-Lizenz-Scans (SBOM), AAR-Anonymisierung/Pseudonymisierung, Freigabeprozesse.	Niedrig-mittel; Nachweis: Compliance-Berichte, Prüfpfade.
R-A12	Field/Umweltbedingungen	Energie-/Temperaturlimits, GPS-Störungen, physische Risiken.	Instabilität, Zeitinkonsistenz, Datenverlust.	Thermal-Alarme, Zeitquellen-Failover, USV-Ereignisse.	USV/Redundanz, Ruggedized-Hardware, alternative Zeitquellen, Verschlüsselung at-rest, Tamper-Erkennung.	Mittel; Nachweis: Site-Abnahmen, Umgebungsprotokolle.
R-A13	Telemetrie-Sättigung/Index-Engpässe	Hoher MELT-Durchsatz, unzureichende Storage-/Index-Strategien.	Anfragen > 2 s, Datenlücken.	Ingest-Lag, Queue-Tiefe, Query-P95.	Backpressure/Sampling, Hot/Warm/Cold-Tiers, Kapazitätsprognosen, priorisierte Pipelines.	Mittel; Nachweis: Sizing-Reports, SLO-Monitoring.
R-A14	Patch-Regression	Änderungen ohne	Instabilität, Downtime.	Fehlerraten nach	Quarantäne --> Staging -->	Niedrig-mittel;

ID	Risiko (Kurzbezeichnung)	Ursache	Wirkung	Indikatoren	Maßnahmen/ Behandlung	Restrisiko & Nachweise
		ausreichende Staging-Prüfung/Feature-Flags.		Rollout, Rollback-Häufigkeit.	Prod, Canary/Blue-Green, verbindliche Rollbacks (Snapshots).	Nachweise: Release-AARs, Rollback-Protokolle.
R-A15	Kompatibilität/Abhängigkeitsfragmentierung	Heterogene Hypervisor-/Treiberstände, Nested-Virt-Einschränkungen.	Laufzeitfehler/Performanceeinbrüche.	Fehlercluster in bestimmten Host-Profilen, Inkompatibilitätswarnungen.	Referenz-Hardware-Matrizen, Abnahmetests je Profil, strikte Versionspins.	Niedrig; Nachweise: Kompatibilitätstabellen, Testprotokolle.
R-A16	Bastion/Jump-Host-Sicherheit	Zugangsdiebstahl, unzureichende Sitzungsaufsicht.	Laterale Bewegungen, Datendiebstahl.	Ungewöhnliche Sitzungsdaten/-zeiten, fehlgeschlagene MFA-Versuche.	MFA offline-fähig, kurzlebige Zugänge, vollständige Sitzungsaufzeichnung, Mikrosegmentierung.	Niedrig-mittel; Nachweise: Access-Logs, Review-Protokolle.
R-A17	Datenschutz/Lerndaten	Personenbezogene Leistungsdaten im AAR/Export.	Datenschutzverstöße, Reputationsschäden.	PII-Funde im Export, unautorisierte Zugriffe.	Anonymisierung/Pseudonymisierung, RBAC-Leserechte, definierte Retention/Deletion, Privacy-Review vor Export.	Niedrig; Nachweise: Export-Checks, Retentionsberichte.

4.6 Referenzarchitektur B – Cloud-native (Kubernetes) mit Service-Mesh & DDS/HLA-Bridge

Die Referenzarchitektur B verfolgt einen Cloud-native-Ansatz, in dem Trainingsdienste und Plattformfunktionen konsequent als containerisierte Workloads auf Kubernetes bereitgestellt werden. Änderungs- und Betriebszustände werden deklarativ modelliert und per GitOps als einzige, versionierte Wahrheitsquelle verwaltet. Damit entstehen reproduzierbare, auditierbare Deployments, bei denen Zustandsänderungen deterministisch über Pull-basierte Controller aus signierten Repositories eingespielt und über Drift-Detektion überwacht werden. Die Durchsetzung von Identitäten und Netzwerkregeln erfolgt über ein Service-Mesh mit mTLS-Verschlüsselung by default und SPIFFE/SPIRE-basierten Service-Identitäten (SVIDs). Dies ermöglicht feingranulare AuthN/AuthZ-Policies (Zero-Trust), kontrolliertes Traffic-Management (Rate-Limits, Circuit-Breaking, Fault-Injection) sowie konsistente Telemetrieerzeugung. Für die Simulations-Interoperabilität nutzt die Architektur DDS-Domänen (Data Distribution Service, Publish/Subscribe) und koppelt bestehende HLA-Ökosysteme über eine DDS/HLA-Bridge, die Datentypen, Ownership und Zeitmechanismen zwischen DDS-Topics und HLA-Objekten/Interaktionen verbindlich abbildet. Damit adressiert diese Variante variabel skalierende Ausbildungsumgebungen mit hohem Automatisierungsgrad, ohne auf die etablierten Simulationsstandards der Partner verzichten zu müssen. Der Offline-/Air-Gap-Betrieb wird durch lokale OCI-Registries, Git-Mirrors und strikte Artefakt-Validierung (Signaturen, SBOM, Provenance) unterstützt.

Das Schichtenmodell folgt vier klar getrennten Ebenen. In der Management- & Orchestrierungsschicht werden Szenarien, Policies und Betriebsartefakte als Code geführt (GitOps), durch Admission-/Policy-Controller geprüft und per Controller synchronisiert. Katalog, Orchestrierung (Run-Lebenszyklus, Event-Injection), AAR-Erzeugung sowie IdP/PKI-Dienste sind hier verankert. Die Simulations-/Übungsdienste arbeiten in DDS-Domains und stellen Traffic-/Protokoll-Generatoren, Netzemulation (Latenz/Jitter/Loss) und HIL-Adapter bereit; die DDS/HLA-Bridge realisiert föderationsfähige Sichten und Zeit-/Ownership-Semantik in Richtung HLA. Die Trainings-Applikationen umfassen Hands-on-Portale, Scoring/Flag-Services, Lernpfade/Guided Labs und Blue/Red/Purple-Team-Werkzeuge. Die Infrastrukturschicht stellt Kubernetes-Cluster mit CNI-basierter Segmentierung (NetworkPolicies, optional eBPF), Storage-Klassen, Ingress/Egress-Gateways und Mesh-Control-Plane bereit. Diese strikt getrennte Verantwortungszuordnung verbessert Testbarkeit, Auditierbarkeit und Fehlereindämmung.

Isolations- und Multitenancy-Konzept. Jede Übungsrunde (Run) wird in einem eigenen Namespace mit zugehörigen NetworkPolicies, Ressourcenquoten und LimitRanges betrieben; identitätsgebundene Mesh-Regeln (SVID-basiert) erzwingen Least-Privilege-Kommunikation zwischen Diensten. Zeitkritische Steuerpfade (z. B. Orchestrierungsbefehle, Scoring-Events) erhalten explizite Latenzbudgets und priorisierte Queues, während Bulk-Telemetrie über dedizierte Pipelines fließt. Optional wird die Mandantentrennung auf Unterlay-Ebene durch VRF/VLAN-Segmente verstärkt (z. B. an Edge-Switches oder per dediziertem Workernetz), um physisch-logische Grenzen für besonders sensible Runs zu etablieren. Cleanup-Routinen (TTL-Controller, Garbage-Collection) verhindern Artefaktdrift und sichern reproduzierbare Neustarts.

Service-Mesh-Absicherung und Betriebsfunktionen. Das Mesh liefert mTLS-Verschlüsselung auf Transportebene, beidseitige Authentisierung via SPIFFE-SVIDs und richtlinienbasierte Autorisierung (Service-zu-Service, Namespace-übergreifend). Traffic-Shaping (Rate-Limit, Outlier-Detection, Circuit Breaking) schützt zeitkritische Trainingspfade; Fault-Injection kann didaktisch eingesetzt werden (z. B. Paketverlust, Verzögerungen), bleibt aber durch Szenario-Policies begrenzt. Telemetrie (Metriken, Traces, Logs) wird konsistent pro Run/Namespace erhoben und über einen OTel-Collector write-controlled in die Observability-Zone exportiert; Rückkanäle in

Übungszonen sind technisch ausgeschlossen. Diese Mechanismen bilden die Grundlage für deterministische Replays und forensisch belastbare AARs.

DDS-Interoperabilität und HLA-Kopplung. Innerhalb einer Übung strukturieren DDS-Domains und -Partitions den Datenraum; Topics und Datentypen werden je Run/Rolle genau benannt, QoS-Profile (z. B. Reliability, Durability, Deadline, LatencyBudget) sichern zeit- und zustandsbezogene Anforderungen. Die DDS/HLA-Bridge mappt Topics auf HLA-Objekte/Interaktionen und übernimmt die Zeitverwaltung/Ownership gemäß HLA-Regeln. Damit werden bestehende HLA-Föderationen weiter nutzbar, während cloud-native Trainingsdienste DDS-basiert skalieren. Kopplungen laufen ausschließlich über föderationsfähige Gateways (Mesh-East/West, DDS-Router), sind mTLS-gesichert, zweckgebunden und zeitlich limitiert; Export-/Import-Sichten sind als Policies-as-Code versioniert und vor Aktivierung schema-validiert. Eine gemeinsame Run-ID und eine lokale Zeitquelle (NTP/GPS) gewährleisten Konsistenz, Drift wird überwacht und im AAR markiert.

GitOps-Betrieb, Artefakt-Sicherheit und Air-Gap. Alle Zustände—von Cluster-Baselines (Terraform/Ansible) über Kubernetes-Manifeste (Helm/Kustomize) bis zu Szenario-Definitionen—werden signiert versioniert und über Pull-basierte GitOps-Controller synchronisiert. OCI-Artefakte (Container-Images, Charts) liegen in einer lokalen Registry mit Signatur- (z. B. Cosign) und SBOM-Pflicht; Importe müssen eine Quarantäne mit Signatur-/Hash-Prüfung, SBOM-Abgleich und Offline-Malware-Scan passieren. Provenance-Metadaten dokumentieren, wer wann mit welchen Eingaben gebaut hat; nur signierte Commits/Tags werden aus dem Git-Mirror synchronisiert. Der Disconnect-Test (≥ 24 h) ist Pflichtbestandteil der Abnahme: Weder Control-Plane noch Workloads dürfen Outbound-Abhängigkeiten außerhalb der genehmigten Gateways aufweisen.

Qualitätsattribute und Betriebskennzahlen. Die Architektur priorisiert Agilität und horizontale Skalierbarkeit bei Wahrung strenger Governance. Bereitstellungszeiten für Standard-Szenarien werden über vorgefertigte Manifest-Bundles und deterministische Pipelines minimiert; Reset-Pfad für Hands-on-Labs bleibt < 60 s (Ziel), Orchestrierungs-Kommandos reagieren < 5 s (P95), und Query-Zeiten in Standard-Dashboards liegen < 2 s (P95). Ressourcenquoten und QoS-Einstufungen (Requests/Limits, PriorityClasses) schützen zeitkritische Pfade gegen Noisy-Neighbor-Effekte; Autoscaling (HPA/VPA) ist erlaubt, aber durch Szenario-Budgets begrenzt, um Reproduzierbarkeit zu sichern. Backups/DR umfassen Etcd-Snapshots, Git-Mirrors und Registry-Versionen (WORM-Tiers); Zielwerte sind $RTO \leq 2$ h für zentrale Control-Plane-Dienste und $RPO \leq 15$ min für Konfiguration/Metadaten.

Einsatzspektrum und Trade-offs. Die Variante eignet sich für SOC/NOC-Trainings, Cyber-Range-Szenarien und Hands-on-Labs mit hoher Parallelität und variabler Last. Vorteile sind schnelle Iteration, feingranulare Steuerbarkeit (Policies, Traffic, Identitäten) und nahtlose Telemetrie. Dem stehen erhöhte Komplexität (Service-Mesh-Betrieb, GitOps-Disziplin, Multi-Cluster-Sichten) und strenge Supply-Chain-Anforderungen gegenüber (signierte OCI-Artefakte, SBOM/Provenance). Die Architektur mitigiert diese Risiken durch Policies-as-Code, Quarantäne-Importe, deterministische Rebuilds, Restore-Drills und föderationsspezifische Schema-/Kompatibilitätstests.

4.6.1 Übersicht & Bausteine

Die Referenzarchitektur B priorisiert eine elastische, cloud-native Bereitstellung und Steuerung von Trainingsumgebungen. Grundlage ist ein Vier-Schichten-Modell, das Verantwortlichkeiten und Schnittstellen klar trennt und dadurch Wiederholbarkeit, Isolation und Prüfbarkeit erhöht. Auf der obersten Schicht „Management & Orchestrierung“ werden Szenarien, Policies und Betriebsartefakte als Code erfasst, syntaktisch/semantisch geprüft und über GitOps-Controller deterministisch synchronisiert; hierzu zählen die Ereignisinjektion im Run-Lebenszyklus, die rollenbasierte Zugriffskontrolle auf Basis eines lokalen Identitätsdienstes (IdP/PKI mit

SPIFFE/SPIRE-Identitäten), die gesicherte Bereitstellung aus lokalen Registries und Git-Mirrors sowie die Erstellung von After-Action-Reports (AAR). Die Schicht der „Simulations-/Übungs-Dienste“ stellt generische Mechanismen bereit, um Protokoll- und Verkehrsmuster zu erzeugen und Netzcharakteristika wie Latenz, Jitter und Paketverlust gezielt zu emulieren; Simulationsdatenflüsse folgen dem Publish/Subscribe-Paradigma in DDS-Domänen. Optional werden Adapter für OT-Protokolle und Hardware-in-the-Loop unter strikten Guards eingebunden, während eine DDS/HLA-Bridge Daten- und Zeitsemantik gegenüber HLA-Föderationen standardkonform abbildet. Darauf aufbauend bieten „Trainings-Applikationen“ die didaktischen Frontends: Hands-on-Portale mit automatischem Scoring (z. B. Flag-Abnahme), Lernpfade mit geführten Hinweisen sowie Werkzeuge für Blue-, Red- und Purple-Team-Abläufe; die Applikationen sind pro Run isoliert und durch Service-Mesh-Policies abgesichert. Die Basisschicht „Infrastruktur (Compute/Storage/Netz)“ stellt Kubernetes-Cluster mit CNI-gestützter Segmentierung (NetworkPolicies, optional eBPF), Storage-Klassen und Ingress/Egress-Gateways bereit; Service-Mesh-Control-Planes erzwingen mTLS-by-default, und dedizierte föderationsfähige Gateways entkoppeln Inter-Site-Verbindungen von den Trainingssegmenten.

Die Kernkomponenten dieser Variante sind auf Offline-Betrieb und Nachweisbarkeit ausgelegt. Kubernetes-Cluster mit eindeutig versionierten Node-Profilen und deterministischen Node-Images ermöglichen reproduzierbare Zustandsübergänge und kurze Wiederanlaufzeiten; etcd-Snapshots und deklarative Manifeste sichern die Rekonstitution der Control-Plane. Ein lokaler OCI-Registry-Mirror für Container-Images und Charts erzwingt Signatur- und SBOM-Prüfungen, während ein lokaler Git-Mirror den Szenario- und Infrastruktur-Code (inklusive ADRs) mit signierten Tags/Merges verwaltet; GitOps-Controller synchronisieren ausschließlich geprüfte und signierte Commits. Die Service-Mesh-Control-Plane stellt mTLS, beidseitige Authentisierung über SPIFFE-Identitäten und Zero-Trust-Policies bereit; Traffic-Shaping und Fault-Injection sind kontrolliert für didaktische Zwecke einsetzbar. Der Observability-Stack erfasst Metriken, Events, Logs und Traces (MELT) run-gebunden und zeitlich konsistent; eine lokale Zeitquelle (NTP/GPS) stellt die deterministische Stempelung sicher. Eine offline-fähige PKI/CA unterstützt Schlüssel-Lebenszyklen, kurzlebige Service- und Föderations-Zertifikate und Offline-CRLs; föderationsfähige Gateways koppeln DDS-Domänen und HLA-Föderationen ausschließlich über zweckgebundene, zeitlich limitierte Strecken. Ein streng konfigurierter Bastion-Zugang dient als kontrollierter Einstiegspunkt mit lückenloser Protokollierung und definierten Break-Glass-Prozeduren. Zusammengenommen stützen diese Bausteine die geforderte Reproduzierbarkeit, Isolierbarkeit und Auditierbarkeit im air-gapped, cloud-nativen Betrieb.

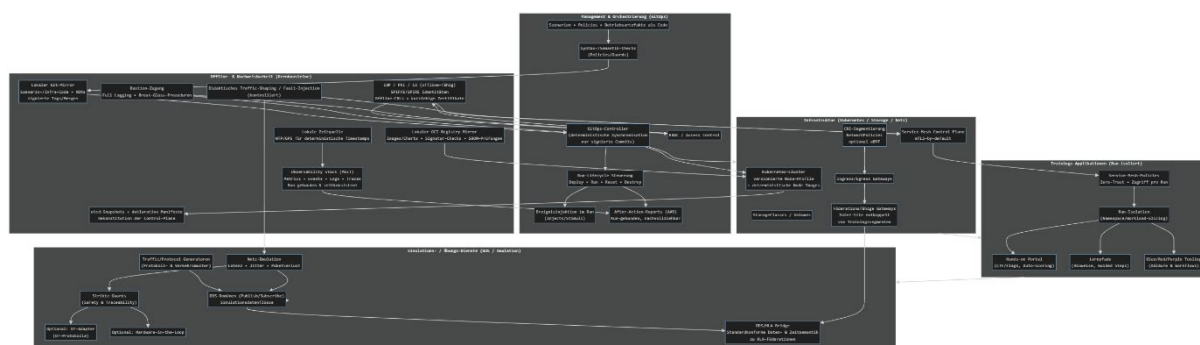


ABBILDUNG 18 ARCHITEKTUR B ÜBERSICHT DER BAUSTEINE

4.6.2 Technologie-Stack und Plattformkomponenten

In dieser Referenzarchitektur kann folgender nachfolgender Technologie-Stack verwendet werden. Ziel ist es, die im vorhergehenden Abschnitt dargestellten Schichten und Bausteine mit konkreten Technologie-Kategorien zu unterlegen und damit ein konsistentes, cloud-natives Plattformprofil zu

skizzieren. Wie bei Referenzarchitektur A handelt es sich nicht um eine verbindliche Produktauswahl, sondern um ein Technologie-Profil, das als Grundlage für nachgelagerte Beschaffungs- und Detaildesign-Entscheidungen dient.

Der Technologie-Stack ist so ausgelegt, dass er folgende, für Referenzarchitektur B charakteristische Ziele unterstützt:

- berechenbare, elastische Bereitstellung containerisierter Workloads auf Kubernetes,
- deklarative Steuerung aller relevanten Zustände (Szenarien, Infrastruktur, Policies) via GitOps,
- Zero-Trust-Kommunikation über ein Service-Mesh mit mTLS-by-default und SPIFFE/SPIRE-Identitäten,
- Simulationsinteroperabilität über DDS-Domänen und eine DDS/HLA-Bridge,
- Offline-/Air-Gap-Betrieb durch lokale Registries, Git-Mirrors und strikte Supply-Chain-Kontrollen,
- durchgängige „Everything-as-Code“-Ausrichtung inklusive Policies- und Controls-as-Code.

Der folgende Überblick fasst die zentralen Technologie-Kategorien zusammen und ordnet ihnen beispielhafte Komponenten zu.

TABELLE 8 TECHNOLOGIE-STACK REFERENZARCHITEKTUR (CLOUD-NATIVE)

Kategorie	Technologie-Profil	Rolle in Referenzarchitektur	Besondere Aspekte in RA
Kubernetes-Cluster & Nodes	Upstream-Kubernetes oder gehärtete Distribution, deterministische Node-Images, Profil-Templates	Ausführungsschicht für containerisierte Plattform- und Übungsdienste	Reproduzierbare Cluster-States, kurze Wiederanlaufzeiten, klar definierte Node-Profile
Container-Netzwerk (CNI)	CNI-Plugin mit NetworkPolicies, optional eBPF-basiert; Ingress-/Egress-Gateways	Segmentierung und Mandantentrennung auf Pod-/Namespace-Ebene	Namespaces + NetworkPolicies als primäre Isolation; Ergänzung durch VRF/VLAN im Underlay möglich
Service-Mesh & Identität	Service-Mesh mit mTLS-by-default; SPIFFE/SPIRE für Service-Identitäten (SVIDs)	Zero-Trust-Kommunikation, feingranulare AuthN/AuthZ und Traffic-Steuerung	SVID-basierte Policies, Fault-Injection für Trainingszwecke, Telemetrie auf Mesh-Ebene

Kategorie	Technologie-Profil	Rolle in Referenzarchitektur	Besondere Aspekte in RA
GitOps & Konfigurationsverwaltung	Git-Mirrors, GitOps-Controller (Pull-basiert), Kustomize/Helm, Policy-/Admission-Controller	Deklarative Steuerung von Konfiguration, Szenarien und Policies	Nur signierte Commits/Tags als Quelle; Drift-Detektion, automatisierte Rollbacks
Infrastruktur-IaC & Basis-Setup	Terraform für Infrastruktur (Compute/Netz/Storage), Ansible für Basis-OS/Cluster-Bootstrap	Bereitstellung und Pflege der K8s-Cluster, Storage- und Netzbasiskonfigurationen	Vollständig als Code beschrieben, reproduzierbare Cluster- und Zonenaufbauten
OCI-Registry & Artefakt-Supply-Chain	Lokale OCI-Registry für Images/Charts, SBOM-/Signatur- und Provenance-Prüfung, Quarantäne-Tiers	Versorgung der Plattform mit Container-Images, Charts und Basis-Artefakten	Signaturpflicht, SBOM-Prüfung, WORM-Tiers; Offline-Imports mit definierter Quarantäne-Pipeline
DDS-Stack & DDS/HLA-Bridge	DDS-Middleware/Router, DDS-Domänen, DDS/HLA-Bridge	Simulationsdatenbus und Kopplung zu bestehenden HLA-Föderationen	Formalisierte Topic-/Typen-Mappings, Ownership- und Zeitharmonisierung zwischen DDS und HLA
Simulations- & Übungsdienste	Containerisierte Generatoren, Netzemulation, HIL-Adapter, Protokoll- und Traffic-Engines	Bereitstellung der eigentlichen Übungs- und Simulationslast	Pro Run isolierte Namespaces, Ressourcenkontingente, Mesh-Policies zur Kontrolle der Pfade
Trainings-Applikationen	Hands-on-Portale, Scoring-/Flag-Services, Lernpfade, Blue/Red/Purple-Team-Werkzeuge	Didaktische Frontends und Bewertungslogik	Multi-Tenancy über Namespaces/Identitäten; Integration in Szenario- und AAR-Workflows
Observability / MELT	OTel-Collector, Zeitreihendatenbank, Log-Store, Tracing-	Erfassung und Auswertung von Metriken, Events,	Write-controlled Observability-Zone, Query-SLOs (z. B. <

Kategorie	Technologie-Profil	Rolle in Referenzarchitektur	Besondere Aspekte in RA
	Komponente, Dashboarding	Logs, Traces (MELT) pro Run/Namespace	2 s P95), Run-ID-basierte Telemetrie
Identity & Access Management	Lokaler IdP/PKI, RBAC (Cluster/Namespace), Mesh-Identitäten, ggf. Bastion-Hosts	Authentisierung und Autorisierung von Nutzenden, Diensten, Administrationspfaden	Kurzlebige Credentials, Rollenmodelle (z. B. Trainer:in, Beobachter:in, Plattform-Ops), Audit-Logs
Sicherheits- & Policy-Stack	Admission-/Policy-Controller (z. B. OPA/Gatekeeper-ähnlich), PodSecurity-/NetworkPolicies	Technische Durchsetzung von Sicherheits- und Governance-Richtlinien auf K8s-Ebene	„Policies-as-Code“ mit Review/CI-Pipeline, Default-Deny, Egress-Kontrolle
Management-, Backup- & DR-Werkzeuge	Cluster-Management, Backup-/Restore (inkl. etcd), Monitoring von SLOs/Synchro-Lags	Unterstützung von Betriebs-, Wiederherstellungs- und DR-Prozessen	Geprobte DR-Runbooks, dokumentierte RTO/RPO, regelmäßige Restore-/Disconnect-Drills

Kubernetes- und Infrastrukturschicht

Die Kubernetes-Cluster bilden die technische Basis der Referenzarchitektur B. Gehärtete Node-Images und klar definierte Node-Profile sorgen dafür, dass Control-Plane- und Worker-Knoten reproduzierbar aufgebaut und aktualisiert werden können. Die Provisionierung der Cluster erfolgt deklarativ über IaC-Werkzeuge; Netz- und Storage-Ressourcen werden dabei so modelliert, dass Namespaces, Storage-Klassen und Ingress-/Egress-Gateways direkt an das Zonenmodell der Plattform anschließen. Die Kombination aus Cluster-Rollen, Node-Profilen und Ressourcenquoten ermöglicht es, unterschiedliche Trainings- und Föderationsszenarien in getrennten Clustern oder logisch separierten Pools abzubilden, ohne den Betrieb zu fragmentieren.

GitOps-, Artefakt- und Supply-Chain-Management

Sämtliche relevanten Zustände – von Infrastruktur- und Plattformkonfiguration über Szenario-Bundles bis hin zu Policies – werden in Git-Repositories verwaltet. GitOps-Controller synchronisieren diese Zustände ausschließlich pull-basiert und nur aus signierten, geprüften Branches und Tags. Änderungen durchlaufen eine definierte Pipeline mit statischen Checks, Policy-Validierungen und optionalen Staging-Deployments, bevor sie produktiv übernommen werden. Lokale Git-Mirrors und OCI-Registries stellen sicher, dass der Betrieb auch in stark eingeschränkt angebundenen oder vollständig vom Internet entkoppelten Umgebungen aufrecht erhalten werden kann. Die Supply-Chain-Kontrollen (Signaturen, SBOMs, Provenance-Metadaten)

ermöglichen die Nachvollziehbarkeit von Artefakt-Herkünften und bilden die Grundlage für Quarantäne- und Rollback-Pfade.

Service-Mesh, Identitäten und Netzwerkpolitik

Das Service-Mesh ergänzt die grundlegende CNI-Segmentierung um eine Zero-Trust-Komponente auf Workload-Ebene. Jede Service-zu-Service-Kommunikation erfolgt mTLS-verschlüsselt; SPIFFE/SPIRE-basierte Service-Identitäten (SVIDs) erlauben feingranulare Autorisierungsregeln über Namespaces und Cluster hinweg. Traffic-Shaping-Funktionen (Rate-Limits, Circuit-Breaking, Outlier-Detection) schützen zeitkritische Trainingspfade vor Überlast, während gezielte Fault-Injection für didaktische Zwecke eingesetzt werden kann. NetworkPolicies und Mesh-Policies werden als Code verwaltet und über Admission-Controller konsistent durchgesetzt, sodass unerwünschte Kommunikationspfade früh erkannt und blockiert werden.

DDS-Stack, Trainingsapplikationen und Observability

Die Simulations- und Übungsdienste operieren auf DDS-Domänen, in denen Datenflüsse gemäß Publish/Subscribe-Paradigma organisiert sind. DDS-Router und eine DDS/HLA-Bridge stellen die Interoperabilität zu HLA-basierten Föderationen her und bilden Daten-, Ownership- und Zeitmodelle verbindlich ab. Trainingsapplikationen – etwa Hands-on-Portale, Scoring-Dienste und Team-Werkzeuge – greifen auf diese Datenströme zu und liefern die didaktischen Oberflächen für Trainer:innen und Teilnehmende. Die Observability-Schicht erfasst Metriken, Events, Logs und Traces aus Kubernetes, Mesh und Workloads run-gebunden und exportiert sie write-controlled in eine dedizierte Observability-Zone. Dashboards und Auswertungen sind auf die im Anforderungskatalog definierten SLOs ausgerichtet (z. B. Bereitstellungszeiten, Orchestrierungs-Latenzen, Query-Antwortzeiten) und unterstützen sowohl die operative Steuerung als auch die Erstellung forensisch belastbarer After-Action-Reports.

Der hier skizzierte Technologie-Stack definiert ein konsistentes, cloud-natives Plattformprofil für Referenzarchitektur B. Er trägt der Priorisierung von Agilität, Elastizität und feingranularer Governance Rechnung, ohne die Anforderungen an Air-Gap-Betrieb, Nachweisbarkeit und Interoperabilität zu vernachlässigen, und bildet damit die Grundlage für Aufbau, Betrieb und Weiterentwicklung der Variante B sowie für den systematischen Variantenvergleich mit Referenzarchitektur A.

4.6.3 Integrations- & Föderationskonzept

Interoperabilität wird domänenspezifisch über DDS realisiert, während die Kopplung zu etablierten HLA-Umgebungen durch eine dedizierte Bridge erfolgt. Auf DDS-Seite strukturieren Domains/Partitions den Austausch; Themen (Topics) werden pro Übung/Rolle benannt und in Policies als Export-/Import-Sichten fixiert. Die DDS/HLA-Bridge mappt Topics/Datentypen auf HLA-Objekte/Interaktionen und setzt Zeit-/Eigentumsmechanismen entsprechend der Föderationsregeln um. Für netzseitige Trennung sind dedizierte Föderations-Gateways vorgesehen; Austauschpfade sind mTLS-gesichert, zweckgebunden und zeitlich limitiert. Im Mesh erzwingen AuthN/Z-Policies (SPIFFE-Identitäten) den principle-of-least-privilege.

Föderierte Übungen können multi-cluster und multi-site betrieben werden. Service-Mesh-Gateways etablieren East/West-Verbindungen zwischen Clustern (nur für freigegebene Services/Topics); DDS-Domains können über Relay/Router gekoppelt werden. Vor jeder Koppelung werden Schema- und Policy-Kompatibilität validiert. Zeitkonsistenz stützt sich auf lokale Zeitquellen und eindeutige Run-IDs; verbleibende Drift wird überwacht und in AARs kenntlich gemacht. Für Realintegration (HIL) werden Proxies/Adapter bereitgestellt, deren Pfade strikt gedrosselt und protokolliert werden; Ereignisse aus Realquellen sind im Datenstrom eindeutig markiert.

4.6.4 Deploy-/Infrastruktur-View

Referenz-Topologien: (a) Single-Cluster-Site (Entwicklung/Abnahme/Trainingsbetrieb mit mittlerer Parallelität), (b) Multi-Cluster-Multi-Site (verteilte Übungen, föderierte Szenarien), (c) Edge/Field-Cluster (kompakter Kubernetes-Stack, z. B. k3s, mit lokalen Registries und Git-Mirrors). In allen Varianten werden Übungsrunden über Namespaces und NetworkPolicies isoliert; sensible Pfade (Föderation/HIL) verlaufen über dedizierte Gateways. Ingress/Egress-Kontrolle wird am Cluster-Rand und im Mesh durchgesetzt; Observability-Daten fließen write-controlled in eine gesonderte Telemetrie-Zone.

Netzdesign: Die Trennung erfolgt primär über Namespaces (L7-Identitäten via Mesh) und CNI-basierte NetworkPolicies (L3/L4, optional eBPF-beschleunigt). Für harte Mandantentrennung zwischen Runden/Tenants werden VRFs/VLANs an den Edge-Switches oder über Underlay-Segmente genutzt. East/West-Gateways verbinden Cluster/Standorte über mTLS-gesicherte Strecken; Export/Import-Sichten sind als Policies-as-Code versioniert. Guard-Funktionen prüfen Protokollkonformität, Raten und Inhaltsfilter vor Übergang in Föderations- oder HIL-Segmente.

4.6.5 IaC & Betriebsartefakte

Die in Kapitel 4.5.5 beschriebenen Grundprinzipien für IaC und Betriebsartefakte (deterministische, auditierbare und air-gap-fähige Lieferkette; Signaturen, SBOM/Provenance; Quarantäne → Staging → Produktion; Disconnect-Test ≥ 24 h; RTO/RPO-Ziele) gelten unverändert. Für die cloud-native Referenzarchitektur B ergeben sich im Schwerpunkt container- und GitOps-spezifische Anpassungen, die im Folgenden zusammenhängend ausgeführt werden (vgl. 5.4 für das generische Verfahren).

Die Repository- und Artefaktstruktur erweitert die in 5.4 skizzierte Dreiteilung um Kubernetes-Sichten und Policy-Bundles. Neben /infra/terraform (Clusterknoten, Storage-Pools, Netz-/VRF-Segmente, Gateways) und /config/ansible (Knoten- und OS-Härtung inkl. Container-Runtime, Bootstrap von Mesh/OTel-Agenten) führt B ein eigenes /manifests für Helm-Charts und Kustomize-Overlays ein. Release-fähige Manifest-Bundles werden signiert, renderbar (kustomize build/helm template) und diff-fähig gehalten. Ergänzend werden /policies (OPA/Gatekeeper oder Kyverno) als Policies-as-Code versioniert, die Admission-Regeln, Netz-/Identitäts-Policies und Ressourcenbudgets durchsetzen. Der Bereich /images ist zweigeteilt: /images/node beschreibt deterministische Node-Images (Knotenprofile inklusive Kernel/CRI/Härtung), /images/base enthält reproduzierbare Basis-Container als Ausgangspunkt für Plattform- und Trainingsdienste. Alle Repositories unterliegen signierten Merges/Tags und Vier-Augen-Freigaben; sensible Variablen verbleiben, wie in 5.4, in einem offline geführten Secrets-Tresor.

Die „Golden-Artefakt“-Politik wird in B auf zwei Ebenen angewandt: Node-Images (für die Control-/Worker-Ebenen) und Golden Base Containers (OCI-Images) ersetzen die OVA-Golden-Images aus A (vgl. 4.5.4). Beide Artefaktklassen werden aus fixierten Mirrors mit Version-Pins und deterministischen Build-Parametern erzeugt, minimal gehalten (Diensteminimierung, konsistente Crypto-Policies) und verpflichtend mit SBOM, Prüfsumme und Signatur versehen. Die Provenance (Wer/Wann/Womit) wird pro Build attestiert. Freigaben setzen Härtings-Benchmarks, Offline-Malware-Scans, Start-/Dienstetests und Self-Checks zur Netzisolation voraus; der Dreifach-Rebuild-Nachweis (≥ 3 identische Artefakte mit Hash-Gleichheit) bleibt Voraussetzung für Promotion in Write-Once-Klassen der lokalen Registry/Chart-Mirror (vgl. 4.5.4, Golden-Image-Freigabe).

Das Versions- und Signaturkonzept übernimmt die in 4.5.4 geforderte Semver-Disziplin und erweitert sie um OCI-Artefakte: Container-Images und Charts sind signiert und in der Registry nur

über Digest-Pins referenziert; GitOps-Controller synchronisieren ausschließlich signierte Commits/Tags. Admission-Ketten prüfen zusätzlich Schema/Policy-Konformität (kubecorn, OPA/Kyverno), Label/Annotation-Disziplin, Ressourcengrenzen und Netz-/Identitäts-Policies (Mesh-mTLS, SVID-basierte Regeln). Widerrufe von Schlüsseln erfolgen offline (CRLs); betroffene Artefakte werden sofort gesperrt und aus Staging zurückgezogen (vgl. 4.5.4, Widerrufsprozess).

Der Offline-Patchprozess folgt unverändert dem Stufenmodell aus 5.4 (Quellen-Snapshot außerhalb der Übungsnetze; Quarantäne-Import mit Signatur/Hash/SBOM-Prüfung und Offline-Scan; Staging-Validierung; Promotion in Produktion). Cloud-native Besonderheiten sind: die Staging-Validierung in einem Test-Cluster via GitOps-Sync mit pausierbaren Sync-Fenstern, der Registry-Snapshot (WORM-Tier) und die Digest-gebundene Promotion (kein Retagging ohne neue Signatur). Leistungsproben messen neben Provisionierungszeit (< 30 min für eine Standard-Range) und Orchestrierungs-Latenzen (< 5 s P95) auch GitOps-Sync-Latenz und Admission-Fehlerraten. Der Disconnect-Test (≥ 24 h) bleibt verbindlich und überwacht explizit, dass weder Control-Plane noch Workloads Outbound-Abhängigkeiten außerhalb genehmigter Gateways besitzen.

Die IaC-Pipeline ist analog zu 4.5.4 in Validierung, Plan/Build, Test, Anwendung, Sign/Release und Archivierung gegliedert, nutzt jedoch B-spezifische Prüfer. In der Validierung sichern Formatter/Linter (terraform fmt/validate, helm lint, kustomize vet), kubecorn und Policy-Engines (OPA/Kyverno) syntaktische und semantische Korrektheit; Secret-Scanner verhindern Klartextgeheimnisse. In Plan/Build erzeugt Terraform driftfreie Pläne; Node-Images und Basis-Container werden deterministisch gebaut; Ansible läuft im Check-Modus; Kustomize/Helm generieren rendered Manifests für Diff- und Admission-Tests. Die Testphase ergänzt Unit/Molecule- und Infrastrukturtests um ephemere Test-Cluster zur Validierung der Admission-Kette. Die Anwendung erfolgt via GitOps-Sync in Staging mit Zeitbudgets und Health-Checks; bei Abweichungen greift ein automatischer Rollback auf den zuletzt signierten Stand. Abschließend werden Artefakte signiert und mit Release-Notes (Hashes, SBOM-Fingerprints, Provenance) veröffentlicht; alle Zustände/Logs/Prüfberichte werden unveränderlich archiviert (vgl. 4.5.4).

Die Kopplung an Qualitätsziele bleibt identisch zu 5.4: Provisionierung einer Standard-Range < 30 min, Reset-Zeit für Hands-on-Labs < 60 s, Orchestrierungs-Kommandos < 5 s (P95), Dashboard-Queries < 2 s (P95). Zusätzlich werden in B Sync-Lags (GitOps), Policy-Durchsetzungsraten und Noisy-Neighbor-Schutz (QoS- und Priority-Klassen) als SLOs überwacht. AAR-Pakete verlinken, wie in 4.5.4, sämtliche verwendeten Artefakte über Version/Hash/SBOM-Fingerprints und sichern so deterministisches Replay.

Für Wiederherstellung/Re-Konstitution gelten die Vorgaben aus 4.5.4; B ergänzt etcd-Snapshots und Control-Plane-Wiederanlauf. Die Reihenfolge bleibt: Zeitquelle/PKI → Observability-Ingest → Orchestrierung/GitOps-Sync → Simulations-/Trainingsdienste. Zielwerte sind RTO ≤ 2 h (zentrale Control-Plane) und RPO ≤ 15 min (Konfiguration/Metadaten). DR-Drills werden protokolliert und als AAR mit Artefaktbezug archiviert. Sicherheit & Betrieb

4.6.6 Sicherheit & Betrieb

Nachfolgenden wird die sicherheits- und betriebsrelevanten Leitlinien der cloud-nativen Referenzarchitektur B konkretisiert. Die Grundprinzipien bereits in Kapitel 5.5 beschrieben sind (Air-Gap-Fähigkeit, Auditierbarkeit, Evidenzpflicht), gelten unverändert; der Fokus liegt hier auf den Kubernetes-, Service-Mesh- und GitOps-spezifischen Ausprägungen.

4.6.6.1 Zonenmodell und Durchsetzung

Das Zonenmodell unterscheidet Management & Orchestrierung, Trainings-/Tenant-Zonen, Föderation/HIL sowie eine Observability-Zone. Die Mandantentrennung erfolgt primär in



Kubernetes über Namespaces mit NetworkPolicies (CNI, optional eBPF-Beschleunigung) und ResourceQuotas/LimitRanges; identitätsgebundene Mesh-Policies (SPIFFE/SPIRE-SVIDs) erzwingen Zero-Trust-Kommunikation auf L7/L4. Für besonders sensible Runs kann die Trennung im Underlay mittels VRF/VLAN verstärkt werden (vgl. 4.5.3).

Zonenübergänge sind streng kontrolliert:

- Ingress/Egress-Gateways des Service-Mesh terminieren mTLS, erzwingen beidseitige Authentisierung und Policy-Filter (Export/Import-Sichten, Protokoll-/Inhaltsvalidierung, Rate-Limits).
- Föderationspfade (DDS-Router, DDS/HLA-Bridge) sind dedizierten Namespaces und föderationsfähigen Gateways zugeordnet; Strecken sind zweckgebunden und zeitlich limitiert.
- Die Observability-Zone ist write-controlled (OTel-Collector Gateways); read-only erfolgt rollenbasiert über Management.

Deny-by-default gilt am Cluster-Rand (EgressPolicies/Firewalls) und im Mesh. Admission-Controller (z. B. OPA/Gatekeeper, Kyverno) prüfen Policies-as-Code: Schema-Gültigkeit, Label/Annotation-Disziplin, Ressourcengrenzen, PodSecurity-Standards, Netz-/Identitäts-Policies sowie Signaturpflicht für Bundles/Images. Disconnect-Tests (≥ 24 h) belegen Air-Gap-Tauglichkeit (keine Outbound-Abhängigkeiten außerhalb genehmigter Gateways).

4.6.6.2 Härungsleitlinien (Control-Plane, Nodes, Workloads, Mesh, Prozesse)

Control-Plane. Minimaler API-Footprint; Abschaltung unsicherer Kube-APIs; RBAC nach Least-Privilege; etcd-Verschlüsselung at rest; Audit-Logging aktiviert; restriktive Admission-Kette (signierte Manifeste, Policy-Konformität). Kube-Controller/Scheduler sind ressourcenseitig isoliert; Bastion-Zugänge protokolliert (Sitzungsaufzeichnung, „Break-Glass“ zeitlich begrenzt, Vier-Augen-Freigaben).

Worker/Node-Images. Secure/Measured Boot (soweit verfügbar), deterministische Golden Node Images (vgl. 4.6.4), gehärtete Kernel-/Netzparameter, cgroups v2, deaktivierte unnötige Dienste. Container-Runtime restriktiv (keine unsicheren Registries, Rootless/Least-Privilege, Read-only-FS wo möglich). PodSecurity (Baseline/Restricted), seccomp/AppArmor/SELinux, kapselnde Netzpfade (keine HostNetwork/hostPath ohne Begründung).

Workloads. Durchgängig mTLS im Mesh; signierte OCI-Images (Digest-Pins, SBOM), Verifikation in Admission. Verbot privilegierter Container/CAPs ohne ATO (Authority to Operate). Härung von Trainings-Applikationen (z. B. sichere Flag-Services), deterministische First-Run-Hooks nur für Run-spezifische Minimalparameter.

Mesh & PKI. SPIFFE/SPIRE als Identitätsanker; kurzlebige SVIDs/Zertifikate, rotierend und offline widerrufbar (CRLs). Traffic-Shaping (Rate-Limit, Outlier-Detection, Circuit-Breaking) schützt zeitkritische Steuerpfade; Fault-Injection ist ausschließlich szenariogesteuert und begrenzt. Keys/Tokens sind kurzlebig; kein Klartext-Secret in Repos/States (offline-Tresor, versiegelte Bundles).

Lieferkette/Prozesse. GitOps-Disziplin (signierte Commits/Tags, Vier-Augen-Merges), Quarantäne-Importe (Signatur/Hash/SBOM/Offline-Scan) und Determinismus-Nachweise (≥ 3 identische Builds) sind verbindlich (vgl. 4.6.4). Change-Management mit Freeze-Fenstern vor Großübungen; Canary/Blue-Green und Rollback-Pfade (Digest-gebunden) für risikobehaftete Änderungen.



4.6.6.3 Backup/Restore (RTO/RPO) und Re-Konstitution

Schutzobjekte. (i) Konfigurations-/Code-Artefakte: Git-Mirror (Infra/Manifeste/Policies/ADRs), Terraform-States, Registry-Metadaten; (ii) Laufzeit-/Datenartefakte: etcd-Snapshots, AAR-Pakete, Telemetrie/Logs; (iii) Artefakt-Spiegel: OCI-Registry (Images/Charts), DDS/HLA-Konfigurationen. Alle Sicherungen sind verschlüsselt, signiert und auf WORM/Offline-Medien mit dokumentierter Chain-of-Custody abgelegt (GFS-Rotation).

Zielwerte. Konsistent zu 4.5.5/4.6.4: RTO zentrale Control-Plane/Orchestrierung ≤ 2 h, RPO Git/Manifeste/States ≤ 15 min; Retention für AAR/Telemetrie gemäß Policy (z. B. 12–24 Monate). Registry-Snapshots (WORM) sichern OCI-Artefakte digest-gebunden; Key-Material (PKI/Mesh) liegt versioniert mit Offline-CRLs vor.

Wiederherstellungspfad. Reihenfolge: Zeitquelle und PKI/CA $\rightarrow$ Control-Plane (Nodes, etcd-Restore) $\rightarrow$ GitOps-Sync der signierten Bundles $\rightarrow$ Mesh/Observability $\rightarrow$ Simulations-/Trainingsdienste. DR-Runbooks (Bare-Metal bis Applikation) sind verpflichtend; DR-Drills (mind. halbjährlich) liefern Nachweise (Ist-RTO/RPO, Abweichungen) und fließen in AAR/ADR ein. Medienhygiene (Offline-Scan, Signaturprüfung vor Restore) ist dokumentationspflichtig.

4.6.6.4 Monitoring & Logging (Observability/MELT)

Die Observability-Architektur erfasst Metriken, Events, Logs, Traces/Flows (MELT) run-gebunden und zeitkonsistent. OTel-Collector (DaemonSet/Gateways) sammelt Workload-, Mesh- und K8s-Signale und exportiert sie write-controlled in die Observability-Zone; Rückkanäle in Tenant-Zonen sind ausgeschlossen. Sämtliche Datensätze tragen Run-ID und präzise Zeitstempel (lokale Zeitquelle). Index-/Korrelationsdienste sind auf SLO-Ziele getrimmt: Query-Antwortzeiten < 2 s (P95) für definierte Standard-Sichten; Ingest-Lag und Drop-Rate liegen innerhalb definierter Toleranzen.

Sicherheits-/Governance-Sichten umfassen: mTLS-Fehlerraten im Mesh, Admission-Denials (Policy-Verstöße), GitOps-Sync-Lags, Egress-Hits/Policy-Verletzungen, Föderations-Handshake-Fehler (DDS-Router/HLA-Bridge), Timeline-Drift in föderierten Runs. Kapazitäts-/Leistungssichten tracken Ressourcenquoten, Noisy-Neighbor-Indikatoren, Registry-/Index-Tiers (Hot/Warm/Cold) und Backpressure in Telemetrie-Pipelines. Log-Integrität wird über verkettete Hashes, signierte Batches und unveränderliche Ablage (WORM/Append-only) gewährleistet; Exporte werden als signierte AAR-Anhänge bereitgestellt. Datenschutz: Datenminimierung, rollenbasiertes Lesen und Anonymisierungs-/Pseudonymisierungsmodi für AAR/Exports.

Betriebsroutinen beinhalten tägliche Gesundheitschecks (Zeitbasis, Sync-Lag, Ingest-Lag), Policy-Mutationstests (Admission-Regeln), Kapazitätsprognosen sowie SLO-Alarme zu Kernzielen (Provisionierung Standard-Range < 30 min; Reset Hands-on < 60 s; Orchestrierungs-Befehle < 5 s P95). Abweichungen triggern Rollback-/Quarantäne-Pfade oder Policy-Revalidierung; Ergebnisse werden in AARs dokumentiert.

4.6.7 Risiken

Zentrale Risiken umfassen: (i) Mesh-Komplexität und Fehlkonfiguration (Seiteneffekte auf Latenz/Erreichbarkeit), (ii) Container-Image-Sprawl und Supply-Chain-Schwachstellen (unsignierte/undokumentierte Basis-Images), (iii) Multi-Cluster-Drift im GitOps-Betrieb, (iv) Noisy-Neighbor-Effekte und Ressourcenkonkurrenz, (v) DDS/HLA-Bridge-Mapping-Fehler (Schema/Ownership/Timing), (vi) Registry-/Git-Mirror-Kompromittierung, (vii) Control-Plane-Ausfälle. Gegenmaßnahmen: strikte Policies-as-Code (Admission/Gatekeeper), Signatur-/SBOM-Pflicht und Quarantäne-Importe, deterministische Rebuilds, Kapazitäts-/Lasttests

mit ressourcenfester QoS-Einstufung (Request/Limit/Scheduling), Schema-/Kompatibilitätstests für DDS/HLA, mehrstufiges Backup (Etcd/Git/OCI), DR-Runbooks und periodische Restore-Drills.

Der Risikokatalog in der Tabelle 7 listet die wesentlichen Gefährdungen der cloud-nativen Referenzarchitektur (Kubernetes, Service-Mesh, GitOps, DDS/HLA-Bridge) mit Ursache, Wirkung, Indikatoren, Maßnahmen und Restrisiko/Nachweis.

TABELLE 9 RISIKOKATALOG B

ID	Risiko (Kurzbezeichnung)	Ursache	Wirkung	Indikatoren	Maßnahmen/ Behandlung	Restrisiko & Nachweis
R - B 1	Mesh-Komplexität/Misconfiguration	Fehlkonfigurierte mTLS/Peer-Auth, unvollständige SPIFFE-Identitäten, Policy-Lücken.	Unverschlüsselte/unerlaubte Verbindungen, Identitätsverwechslungen, Angriffsflächen-Zuwachs.	mTLS-Handshake-Fehler, ungewöhnliche Allow-Rates, Policy-Bypass in Mesh-/Admission-Logs.	mTLS-by-default, strikte Peer/Request-Auth-Policies, SPIFFE/SPIRE-Health-Checks, Change-Reviews, Canary-Validierung.	Mittel; Nachweis: Mesh-Audit-Logs, Policy-Tests, mTLS-Metriken.
R - B 2	GitOps-Supply-Chain/Drift	Unsignierte Commits/Tags, kompromittierter Git-Mirror, fehlende Provenance.	Manipulierte Manifeste, unerkannte Cluster-Drifts.	Admission-Denials variieren, Reconcile-Spitzen, Signatur-Warnungen.	Nur signierte Commits/Tags, Pull-only GitOps, Quarantäne-Importe, Provenance-Atteste, Vier-Augen-Merges, Digest-Pins.	Niedrigmittel; Nachweis: Signaturprüfungen, Reconcile-Protokolle.
R - B 3	OCI-Registry/Artefakte kompromittiert	Unsigned Images/Charts, kompromittierte Registry, Retagging ohne Freigabe.	Ausführung unsicherer Images, Supply-Chain-Infektion.	Cosign-Fehler, SBOM-Diffs, Digest-Mismatch, unerwartete Pulls.	Signatur-/SBOM-Pflicht, WORM-Tiers, Digest-Promotion, Offline-Scan, Registry-ACL Least-Privilege.	Mittel; Nachweis: Registry-Audits, Signatur-Logs, SBOM-Berichte.
R - B 4	Admission-/Policy-Lücken	Zu lax/fehlerhaft definierte OPA/Kyverno-Regeln, deaktivierte Webhooks.	Unsichere Manifeste gelangen ins Cluster, Rechte/Netzpfad-Eskalation.	Anstieg Admission-Denials nach Fixes, Coverage-Gaps, out-of-policy Deploys.	Policies-as-Code mit Tests, Validating/Mutating Admission aktiv, Coverage-Berichte, CI-Gates, protokollierte	Mittel; Nachweis: Admission-Metriken, Policy-Testläufe.

					s Break-Glass.	
R - B 5	Multi-Cluster-Drift/Split-Brain	Unterschiedliche Bundles/Versionen, GitOps-Sync-Lag, manuelle Hotfixes.	Inkompatible Laufzustände, Föderations-Fehler, Latenzspitzen.	Divergierende Digests, erhöhte Reconcile-Queue, Inkompatibilitätswarnungen.	Einheitliche Channels, Sync-Fenster, Drift-Detection, manuelle Changes verboten, Test-Cluster vor Promotion.	Mittel; Nachweis: Drift-Reports, Digest-Vergleiche.
R - B 6	Noisy-Neighbor/Resource-Konkurrenz	Fehlende/zuniedrige Requests/Limits, unpassende HPA/VPA-Profile.	Latenzspitzen, SLO-Verletzungen (z. B. Orchestrierungs-<5 s).	Throttle/Eviction-Metriken, HPA-Flapping, Queue-Backlogs.	QoS/PriorityClasses, harte Quotas, Lasttests, Ressourcenbudgets je Run, HPA/VPA-Guardrails.	Mittel; Nachweis: SLO-Dashboards, Kapazitätsberichte.
R - B 7	etcd-Korruption/Verlust	Fehlerhafte Snapshots, Storage-Probleme, ungetestete Runbooks.	Control-Plane-Stillstand, Konfigurationsverlust.	Snapshot-Fehler, defekte WALs, Restore-Warnungen.	Regelmäßige Snapshots/Übungen, Verschlüsselung, Integritätschecks, Restore-Drills (RTO ≤ 2 h, RPO ≤ 15 min).	Niedrigmittel; Nachweis: Restore-Protokolle, Prüfsummen.
R - B 8	DNS/Service-Discovery-Ausfälle	CoreDNS-Fehlkonfiguration, Air-Gap-Inkonsistenzen, Zonenkonflikte.	Nicht erreichbare Dienste, erschwerte Triage.	NXDOMAIN/Servfail-Spitzen, Timeout-Metriken, Mesh-503/504.	Deterministische Zonen, lokale Spiegel, Readiness-Gates, Fallback-Resolver, Disconnect-Tests.	Mittel; Nachweis: DNS-Metriken, Testprotokolle.
R - B 9	Mesh-Overhead/Latenz	Sidecar-Kosten, suboptimales Routing/Retry-Loops.	Überschreiten von Latenzbudgets, didaktische Qualität leidet.	P95/P99-Anstieg, erhöhte Retries, Sidecar-CPU-Last.	Per-Pfad-Budgets, Outlier-Detection, Circuit-Breaking, streng begrenzte Ausnahmen.	Mittel; Nachweis: Mesh-SLOs, Profilergebnisse.
R - B 10	DDS/HLA-Bridge-Mapping-Fehler	Falsche Zuordnung Topic↔Objekt, QoS-Mismatch	Inkonsistente Timeline/Interop, Datenverlust/-duplikate.	Bridge-Warnungen, Dropped Samples,	Schema/QoS-Validierung, minimale Export-Sichtungen,	Mittel; Nachweis: Föderations-Log



		h, Ownership-Konflikte.		Drift-Alarme.	Staging-Föderationstests, AAR-Drift-Markierung.	s, AAR-Drifts.
R - B 1 1	Egress-Erosion /Air-Gap-Leckage	Temporäre Ausnahmen bleiben bestehen, transitive Abhängigkeiten.	Außenkommunikation, Angriffsfläche, Compliance-Verstöße.	Egress-Firewall-Hits, Outbound-Versuche im Disconnect-Test.	Deny-by-default, zeitlich limitierte Ausnahmen, regelmäßige Disconnect-Tests (≥24 h), Offline-Spiegel.	Niedrig-mittel; Nachweise: Firewall/Proxy-Logs, Testberichte.
R - B 1 2	Secrets-Exposition	Klartext-Secrets im Repo/State, schwache KMS-Praxis, fehlende Rotation.	Kompromittierte Zugangsdaten /Schlüssel.	Secret-Scan-Findings, Token-Missbrauchsalarme.	Offline-Tresor, versiegelte Bundles, Rotation, Secret-Scanner in CI, kurze TTLs.	Mittel; Nachweise: Scan-Reports, Rotationssprotokolle.
R - B 1 3	Node-Image-/Kernel-Drift	Uneinheitliche Knotenprofile, veraltete Kernel/Runtimes.	Inkompatibilitäten, Performance-/Sicherheitsprobleme.	Uneinheitliche Labels, Crash-Loops, Kernel-Warnungen.	Golden Node Images, Rebuild-Takt, Profil-Abnahmen, restriktive Runtime-Policies.	Niedrig; Nachweise: Profil-Matrizen, Abnahmen.
R - B 1 4	Admission-Pipeline-Ausfall	Controller-Fehler/Fehlkonfiguration, Bypass-Fenster.	Unsichere Deployments im Cluster.	Sinkende Admission-Rate, Webhook-Fehler, Policy-Misses.	HA-Webhooks, Fail-Closed, synthetische Tests/Watchdogs.	Mittel; Nachweise: Webhook-Status, Synthetische-Checks.
R - B 1 5	PKI/SVID-Ablauf/Rotation (offline)	Abgelaufene CRLs/Zertifikate, fehlerhafte Rotation.	mTLS-Ablehnungen, Partitionierung.	Zertifikatswarnungen, Handshake-Fehler-Spitzen.	Kurzlebige Zertifikate, Rotationskalender, Dual-Control, Rollover-Drills; Offline-CRLs.	Mittel; Nachweise: Key-Inventar, Drill-AA-Rs.
R - B 1 6	Observability-Sättigung/Backpressure	OTel-Collector überlastet, fehlende Tiers, zu feine Traces.	Datenverlust, Query->2 s, Triage-Lücken.	Ingest-Lag, Queue-Tiefe, Dropped-Samples, P95-Anstieg.	Sampling/Rate-Limit, Hot/Warm/Cold-Tiers, Priorisierung, Kapazitätsprognosen.	Mittel; Nachweise: OTel/Index-Metriken, SLO-Reports.



R - B 1 7	HIL-Adapter/hostNetwork-Exposition	Adapter mit Host-Netz, unzureichende Guards.	Seiteneffekte auf Underlay/Übungsnetze, Datenabfluss.	HostNetwork-Pods, Traffic außerhalb Guards, Alerts.	Verbot hostNetwork ohne ATO, Guard-Durchsetzung/Rate-Limits, Positiv/Negativ-Tests, Marker „Realquelle“.	Mittel; Nachweis: Guard-Logs, Netzwerk-Checks.

4.7 Variantenvergleich & Entscheidungsvorlage

Dieses Kapitel beschreibt eine methodisch belastbare Vorgehensweise zur Auswahl zwischen den beiden Referenzarchitekturen A (VM-zentriert & HLA/DIS-föderiert) und B (Cloud-native/Kubernetes mit Service-Mesh & DDS/HLA-Bridge). Ziel ist ein nachvollziehbarer, audittierbarer Entscheidungsprozess, der qualitative Anforderungen in messbare Kriterien, gewichtete Bewertungen und risiko-/szenario-adjustierte Empfehlungen überführt. Wo Grundprinzipien identisch sind (Air-Gap-Fähigkeit, Signaturen/SBOM/Provenance, Disconnect-Tests), verweist dieses Kapitel auf die jeweiligen Architekturkapitel, um Redundanzen zu vermeiden.

4.7.1 Entscheidungsrahmen und Fragestellung

Der methodische Rahmen für die Auswahl zwischen den Referenzarchitekturen A (VM-zentriert, HLA/DIS-föderiert) und B (Cloud-native/Kubernetes mit Service-Mesh und DDS/HLA-Bridge) wird hier festgelegt. Im Zentrum steht die Forschungsfrage, unter welchen organisatorischen, technischen und betrieblichen Rahmenbedingungen – insbesondere in Bezug auf Sicherheitslage, Trainingsprofile, organisatorische Reife und Ressourcenverfügbarkeit – die jeweilige Architektur den höheren Nutzwert für den Trainingsbetrieb erbringt, ohne die MUSS-Anforderungen zu verletzen. Als MUSS gelten die Offline-Fähigkeit (Air-Gap-Tauglichkeit ohne funktionale Degradation), die Föderationsfähigkeit über standardisierte Kopplungen, die Reproduzierbarkeit von Bereitstellung und Runs (Determinismus über IaC/Golden Artefakte) sowie die belastbare After-Action-Review-Evidenz inklusive zeitkonsistenter Telemetrie.

Die Entscheidungsfindung erfolgt zweistufig. In der ersten Stufe wird eine Konformitätsprüfung als Gating-Mechanismus durchgeführt. Ziel ist der begründete Ausschluss von Varianten oder Konfigurationen, die die oben genannten MUSS-Kriterien nicht erfüllen. Hierzu zählen etwa fehlende oder nur partiell nachgewiesene Air-Gap-Fähigkeit, unzureichende oder nicht standardkonforme Föderationskopplungen, unklare oder durchlässige HIL-Isolationsgrenzen sowie ein Mangel an IaC-Determinismus, der Rebuild- und Replay-Fähigkeit beeinträchtigt. Nur Architekturausprägungen, die diese Gate-Kriterien vollständig bestehen, werden zur zweiten Stufe zugelassen.

In der zweiten Stufe wird eine Nutzwertanalyse als gewichtete, nachvollziehbare Mehrkriterienbewertung durchgeführt. Grundlage ist ein transparenter Kriterienkatalog (u. a. Sicherheit, Offline-Tauglichkeit, Föderationsfähigkeit, Real-Integration, Skalierung, Time-to-Train, Betriebsaufwand, Kosten), dem prioritätsabhängige Gewichte zugeordnet werden. Für jede zugelassene Architektur werden auf Basis messbarer Indikatoren normierte Teilscores ermittelt und mit den Gewichten zu einem aggregierten Gesamtscore verdichtet. Abschließend werden Sensitivitätsanalysen eingesetzt, um die Stabilität der Empfehlung gegenüber Änderungen in Gewichten und Messwerten zu prüfen, sowie eine Risikoanpassung vorgenommen, die architekturspezifische Eintrittswahrscheinlichkeiten und Auswirkungen relevanter Risiken berücksichtigt. Das Ergebnis ist eine belastbare, audittierbare Entscheidungsvorlage mit klarer Herleitung und dokumentierter Evidenzbasis.

4.7.2 Kriterienkatalog (mit Operationalisierung)

Ziel dieses Abschnitts ist es, die für den Variantenvergleich relevanten Bewertungskriterien in einer strukturierten, ausfüllbaren Form bereitzustellen. Die Tabelle 8 dient als audittierbare Score-Card: Sie verknüpft die inhaltliche Definition jedes Kriteriums mit klaren Messgrößen/Indikatoren, einem gewichteten Nutzwert (Gewicht w_i) sowie den jeweiligen Scores der Referenzarchitekturen A und B.

Anleitung zur Verwendung: (1) Pro Kriterium wird ein Gewichtung w_i festgelegt; die Summe aller Gewichte muss 1,00 ergeben. (2) Die Evidenzquellen (Messungen, Tests, AARs) eingetragen und es muss der Score normiert (0–5) für A und B werden. (3) Multiplizieren des Scores $\times w_i$, um die gewichteten Werte je Architektur zu erhalten. (4) Bilden einer Summe unten (Σ) der gewichteten Werte; diese bildet den aggregierten Nutzwert pro Variante.

Bewertungsskala (0–5): 0 = nicht erfüllt/kontraproduktiv, 3 = erfüllt/angemessen, 5 = exzellent/übertrifft Ziel. Unbekannte oder unsichere Werte werden bis zur Evidenzlage konservativ mit 1 bewertet.

TABELLE 10 SCORE-CARD

Kriterium	Inhalte (Definition)	Messgrößen / Indikatoren	Gewicht (w_i)	Skala (0–5)	Evidenz (Test/AAR)	Score A	Score B	Gew. A	Gew. B
Sicherheit	Segmentierung (VRF/VLAN bzw. Namespace/Network Policies), mTLS/Identitäten (PKI/SPIFFE), Härtung, Policies-as-Code, Log-Integrität, Guards (HIL/Föderation).	Policy-Coverage %, Audit-Befunde, Rate unerlaubter Flüsse/24h, Disconnect-Erfolgsquote.		0–5					
Offline-Tauglichkeit	Betrieb ohne Internet (≥ 24 h), Artefaktspiegel (OVAs/OCI/Charts), CRLs offline, Air-Gap-Prozesse.	Disconnect-Test (Ja/Nein), # externer Abhängigkeiten (Ziel 0), Zeit bis vollständiger Rekonstitution.		0–5					
Föderationsfähigkeit	HLA/DIS (A), DDS/HLA-Bridge (B), Namensraum-/VRF-Isolation, kurzlebige Schlüssel, Export/Import-Sichten.	Erfolgsquote Handshakes, Schema/QoS-Kompatibilität, Timeline-Drift (ms), Mapping-Fehler rate.		0–5					
Real-Integration (HIL)	Adapter/Guards, Rate-Limits, Marker „Realquelle“, Positiv/Negativ-Tests.	#/Schwere Policy-Verstöße (Ziel 0), Latenzbudget-Einhaltung, Testabdeckung HIL-Pfad.		0–5					
Skalierung	Parallele Runden, Mandantentrennung, horizontale/vertikale Skalierung,	Max. parallele Runs ohne Konflikte, P95-Latenz unter Last, Effizienz		0–5					

Kriterium	Inhalte (Definition)	Messgrößen / Indikatoren	Gewicht (w _i)	Skala (0–5)	Evidenz (Test/ AAR)	Score A	Score B	Gew. A	Gew. B
	Noisy-Neighbor-Schutz.	(Runs/Host bzw. /Knoten).							
Time-to-Train (Bereitstellung)	Zeit bis „trainingsbereit“ (Standard-Ränge), Reset-Zeiten (Labs), Orchestrierungs-Latenzen.	Provisionierung < 30 min, Reset < 60 s, Befehls-Latenz < 5 s (P95).		0–5					
Betriebsaufwand	Pflege Images/Container, Policy-Pflege, GitOps-Disziplin, Admission-/Mesh-Komplexität, Tooling.	Personenstunden/Woche, Change-Fehlerrate, manuelle Eingriffe/Monat.		0–5					
Kosten (CapEx/OpEx)	Hardware/Cluster, Lizenzen/Support, Betrieb (Energie/Personal), Schulungen.	TCO-Schätzung/Jahr, Kosten je Trainingsstunde.		0–5					
Summe			1,00					Σ	Σ

4.7.3 Gewichtungsbildung

Die Methodik zur Festlegung der Kriteriengewichte für den Variantenvergleich wird hier beschrieben. Ziel ist es, strategische Prioritäten (z. B. Sicherheit, Offline-Tauglichkeit, Skalierung) nachvollziehbar in numerische Gewichte zu überführen, damit die spätere Nutzwertanalyse (vgl. 7.5) auf klaren, von allen Beteiligten akzeptierten Grundlagen beruht. Die Gewichtungsbildung folgt drei Leitprinzipien: Transparenz (Entscheidungsgründe sind dokumentiert), Partizipation (relevante Rollen sind eingebunden) und Robustheit (Ergebnis bleibt bei moderaten Annahmeänderungen stabil).

4.7.3.1 Zweck und Einbettung

Die Gewichtung w_i bestimmt, welchen Einfluss ein Kriterium auf das Gesamtergebnis hat. Sie verknüpft die in 7.2 operationalisierten Kriterien mit den strategischen Zielen des Trainingsbetriebs. Ohne eine sauber hergeleitete Gewichtung besteht die Gefahr, dass Einzelscores überinterpretiert oder Fehlentscheidungen nicht plausibel erklärbar werden. Die hier festgelegten Gewichte sind Teil der Governance des Projekts und werden als Architecture Decision Record (ADR) dokumentiert (vgl. 7.9).

4.7.3.2 Vorgehensmodell

Die Gewichtungsbildung erfolgt in vier Schritten:

1. Vorbereitung: Konsolidierung des Kriterienkatalogs (7.2), Eliminierung redundanter Kriterien, Klärung der Messgrößen, Bereitstellung eines kurzen „Reader’s Pack“ (Definitionen, Beispiele, Zielmetriken). Qualitätsregel: Jedes Kriterium muss entscheidungsrelevant sein und messbar (bzw. durch belastbare Indikatoren belegbar).



2. Methodenwahl:
1. Swing-Weighting (empfohlen): Praktikabel, intuitiv, gut moderierbar.
2. AHP (optional): Paarweiser Vergleich; geeignet bei kleinerer Kriteriensatzgröße und Bedarf an Konsistenzprüfung.
3. Durchführung (moderierter Workshop): Teilnehmende: Trainer:innen/Übungsleitung, Security, Plattform-Engineering; Moderation durch eine fachlich neutrale Person. Zeitlicher Rahmen: 60–120 Minuten.
4. Dokumentation, Prüfung, Freigabe: Ergebnisse werden als ADR festgehalten (Datum, Teilnehmende, Begründung, Artefakte), anschließend auf Kohärenz und Sensitivität geprüft und freigegeben.

4.7.3.2 Swing-Weighting

Ziel: Die relative Wichtigkeit der Kriterien über den größtmöglichen Nutzen-Sprung (von „sehr schlecht/0“ zu „sehr gut/5“) abzubilden.

Vorgehen:

1. Referenz festlegen: Alle Kriterien zunächst gedanklich auf „0“.
2. Größter Sprung: Welches Kriterium liefert – bei Verbesserung von 0→5 – den größten Nutzen? Dieses erhält 100 Punkte (Referenz).
3. Relativbewertung: Alle übrigen Kriterien erhalten Punkte relativ zu dieser Referenz (z. B. 70, 60, 40 ...).
4. Aggregation:
 1. Individualgewichte je Person separat erheben (vermeidet Gruppendruck).
 2. Median oder geometrisches Mittel zur Gruppenaggregation verwenden (robust gegen Ausreißer).
5. Normalisierung: Punkte je Kriterium auf w_i skalieren, sodass $\sum w_i = 1,00$
6. Plausibilitätscheck: Prüfen, ob Reihenfolge und Abstände die Strategie widerspiegeln (z. B. Sicherheit $\geq$ Offline $\geq$ Föderation ...).
7. Dokumentation: Begründungen pro Kriterium kurz festhalten (Warum ist Sicherheit z. B. wichtiger als Time-to-Train?).

Gute Praxis / Guardrails:

- Mindestgewicht für sicherheitskritische Kriterien (z. B. $w_{\text{Sicherheit}} \geq 0,20$)
- Obergrenze pro Einzelkriterium (z. B. $w_i \leq 0,35$), um Monokausalität zu vermeiden.
- Keine Nullgewichte für MUSS-Kriterien (Offline, Föderation, Reproduzierbarkeit/AAR).

4.7.3.3 Analytic Hierarchy Process (AHP)

Zielsetzung und Einordnung: Der AHP ist ein axiomatisch begründetes Verfahren zur Mehrkriterien-Gewichtung, das qualitative Präferenzen in quantitative Gewichte überführt. Kernidee ist die paarweise Beurteilung von Kriterien auf einer relativen Verhältnisskala (1–9), aus der ein Prioritätsvektor (Eigenvektor) $w = (w_1, \dots, w_n)$ mit $\sum w_i = 1$ abgeleitet wird. AHP ist



besonders geeignet, wenn (i) die Zahl der Kriterien überschaubar ist und (ii) konkurrierende Prioritäten präzise, intersubjektiv überprüfbar abgegrenzt werden sollen.

Mathematische Grundlage: Für n Kriterien wird eine paarweise Vergleichsmatrix $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ gebildet. Die Einträge a_{ij} folgen der Saaty-Skala 1–9 (1 = gleich wichtig; 9 = extrem wichtiger) und sind reziprok ($a_{ji} = 1/a_{ij}$); auf der Diagonalen gilt $a_{ii} = 1$. Der Prioritätsvektor w ergibt sich als normierter Haupteigenvektor des Problems $Aw = \lambda_{\max} \cdot w$. Bei vollständiger Konsistenz gilt $a_{ij} = w_i/w_j$ und $\lambda_{\max} = n$; in der Praxis wird w als beste Approximation aus A gewonnen (Eigenvektormethode oder äquivalent über log-least-squares per geometrischem Mittel der Zeilen).

Konsistenzprüfung: Die Konsistenz der Urteile wird durch den Consistency Index (CI) und die Consistency Ratio (CR) bewertet: $CI = (\lambda_{\max} - n) / (n - 1)$, $CR = CI / RI(n)$.

$RI(n)$ ist der Random Index (mittlere Inkonsistenz zufälliger Matrizen; typische Werte: $RI(3)=0,58$; $RI(4)=0,90$; $RI(5)=1,12$; ...; $RI(10)=1,49$). Akzeptanzkriterium: $CR < 0,10$. Bei Überschreitung sind die Urteile gezielt zu revidieren (Fokus auf jene Paare mit größter Abweichung $|\log a_{ij} - \log(w_i/w_j)|$). Für sehr kleine Matrizen ($n \leq 3$) kann ein strengerer Schwellenwert (z. B. $CR < 0,05$) verwendet werden.

Vorgehensmodell

1. Strukturierung & Definitionen: Kriterien aus Kapitel 4.7.2 finalisieren (Eindeutigkeit, Messindikatoren); jede Position muss entscheidungsrelevant und messbar sein.
2. Paarweise Vergleiche: Für alle $i < j$ ($n(n-1)/2$ Vergleiche) ein Urteil a_{ij} auf 1–9 festlegen; $a_{ji}=1/a_{ij}$.
3. Aggregation:
 - a. AIJ (Aggregation of Individual Judgments, empfohlen): geometrisches Mittel der Matrizen $\rightarrow$ Gruppenmatrix A .
 - b. AIP (Aggregation of Individual Priorities): Eigenvektoren je Person bilden und prioritätsseitig aggregieren.
4. Prioritätenberechnung: Haupteigenvektor w und $\lambda_{\max}$ bestimmen; w auf Summe 1 normieren.
5. Konsistenzanalyse: CI und CR berechnen; bei $CR \geq 0,10$ Urteile gezielt nachkalibrieren.
6. Dokumentation: Matrix/Matrizen, w , $\lambda_{\max}$, CI/CR, Datum/Teilnehmer:innen als ADR festhalten (vgl. Kapitel 4.7.3).

Robustheit und Sensitivität:

- Lokale Sensitivität: Einzelne Urteile a_{ij} um ± 1 Skalastufe variieren und Einfluss auf w messen.
- Globale Sensitivität: Mehrere Urteile gleichzeitig variieren (Monte-Carlo) und ein Konfidenzband für w_i bestimmen.
- Methodenabgleich: Gegencheck mit Swing-Weighting (vgl. Kapitel 4.7.3); starke Divergenzen $\rightarrow$ erneute Moderation.

Einsatzszenario und Grenzen: AHP eignet sich für $n \leq 9$ Kriterien (z. B. der Katalog in Kapitel 4.7.3 mit 8 Kriterien $\rightarrow$ 28 Vergleiche), wenn feine Prioritätsabstufungen oder strittige Abgrenzungen erforderlich sind. Die Anzahl der Vergleiche wächst quadratisch ($n(n-1)/2$); damit steigen

Moderationsaufwand und kognitive Last. Unsicherheit in Urteilen kann zu Overconfidence-Effekten führen; Erweiterungen wie Intervall- oder Fuzzy-AHP sind in solchen Fällen sinnvoll.

Qualitätsregeln (Good Practice)

- Kalibrierung vor Start: Beispiele für 1/3/5/7/9 gemeinsam definieren (Semantik der Stufen im Kontext festlegen).
- Schutz vor Gruppendruck: Erst individuelle Urteile erheben (AIJ), dann aggregieren und Inkonsistenzen moderiert diskutieren.
- Sicherheitsanker: MUSS-Kriterien erhalten Mindestgewichte; rechnerische Ergebnisse dürfen diese nicht unterschreiten.
- Nachvollziehbarkeit: Starke Präferenzen (≥ 7) mit kurzen Sachgründen belegen (Regulatorik, Risikohebel, Evidenz).
- Revisionstrigger: Neue Bedrohungslage, neue Föderationspartner, geänderte Lastprofile – > AHP-Update mit Versionierung.

Einbettung in den Entscheidungsprozess: Der aus AHP abgeleitete Gewichtungsvektor w fließt direkt in die Nutzwertanalyse ein. Die Konsistenzkennzahl CR dient als Qualitätskriterium der gesamten Entscheidung; $CR < 0,10$ ist Voraussetzung für die Freigabe der Gewichte im ADR. Bei späteren Anpassungen (z. B. geänderte Trainingsprofile) wird der AHP-Schritt wiederholt, die Resultate werden versioniert und in der Score-Card nachvollziehbar aktualisiert.

4.7.3.4 Governance und Qualitätssicherung

Die Governance- und Qualitätssicherungsmechanismen für die Gewichtungsbildung und die darauf aufbauende Nutzwertanalyse wird nachfolgend beschrieben. Ziel ist ein transparenter, reproduzierbarer und auditierbarer Prozess, in dem Rollen, Artefakte, Prüfkriterien und Eskalationswege klar beschrieben und nachweisbar eingehalten werden.

Leitprinzipien und Zielbild: Die Festlegung von Kriteriengewichten (vgl. Kapitel 4.7.3) und deren Anwendung folgt drei Leitprinzipien: Transparenz (Entscheidungen und Begründungen sind dokumentiert und nachverfolgbar), Partizipation (alle relevanten Rollen sind angemessen beteiligt) und Robustheit (Ergebnisse bleiben bei moderaten Annahmeänderungen stabil und bestehen Konsistenz- sowie Sensitivitätsprüfungen).

Rollen und Verantwortlichkeiten (RACI): Beteiligte Rollen: Übungsleitung, Trainer:innen, Security, Plattform-Engineering, Moderation (methodisch neutral), Management/Governance sind in der Table 7. Die RACI-Matrix weist pro Aktivität Verantwortlichkeiten zu (R = Responsible, A = Accountable, C = Consulted, I = Informed).

Aktivität	Übungsleitung	Trainer:innen	Security	Plattform-Engineering	Moderation	Management/Governance
Kriterienkatalog pflegen (Definition/Messgrößen)	A	R	C	C	I	I
Evidenz sammeln & verifizieren (Tests/AAR/Disconnect/Föderation/HIL)	C	R	R	R	I	I
Gewichtungsworkshop ansetzen & durchführen	R	C	C	C	A/R	I

Urteilsaggregation & AHP-Berechnung inkl. CR	I	C	C	R	R	I
Sensitivitätsanalyse & Szenario-Gewichte	C	C	C	R	I	I
Review & Freigabe der Gewichte (ADR)	A	C	C	C	I	C
Score-Card aktualisieren (7.2/7.5) & Veröffentlichung	A	C	C	R	I	I
Revision bei Trigger (vgl. unten) & Versionierung	A	C	C	R	I	C
Archivierung/Audit (WORM, Signaturen, Chain-of-Custody)	C	I	R	R	I	A

TABELLE 11 GOVERNANCE RACI

Prozess und Artefakte (Plan–Do–Check–Act) Plan: Konsolidierung des Kriterienkatalogs; Bereitstellung eines Reader's Pack (Definitionen, Messindikatoren, Beispielwerte); Terminierung und Agenda des Gewichtungswshops. Do: Durchführung der Gewichtungsbildung (Swing/AHP), getrennte Einzelurteile, Aggregation (AIJ), Berechnung des Prioritätsvektors und der Konsistenz. Check: Konsistenzprüfung ($CR < 0,10$ als Standard), Sensitivitätsanalyse (Ein-Parameter und Szenario-Gewichte), Plausibilitätscheck gegen strategische Ziele. Act: Freigabe per ADR, Veröffentlichung in der Score-Card (4.7.3), Versionierung/Archivierung und Festlegung von Revisions-Triggern.

Qualitätskriterien und Metriken

- Konsistenz: AHP-Consistency Ratio (CR) $< 0,10$; bei $n \leq 3$ gilt $CR < 0,05$.
- Evidenzabdeckung: ≥ 80 % der Kriterien mit harten Messwerten/Indikatoren (Rest mit Begründung).
- Quorum: Teilnahme mind. einer Person je Rolle (Übungsleitung, Trainer:innen, Security, Plattform-Engineering); Moderation unabhängig.
- Bias-Kontrollen: Einzelurteile vor Gruppendiskussion; Kalibrierungsbeispiele für 1/3/5/7/9; Dokumentation starker Präferenzen (≥ 7) mit Sachgrund.
- Rückverfolgbarkeit: Gewichtungen referenzieren Evidenz (Testprotokolle, AARs, Messreihen) und Versionen.
- Freigabe-Gate: Ohne ADR-Freigabe keine Verwendung in 7.5; Änderungen nur über versionierte Nachtrags-ADRs.

Bias- und Fehlerquellen sowie Gegenmaßnahmen: Group-Think, Anker- und Verfügbarkeitsheuristiken sowie Status-quo-Bias werden durch getrennte Erhebung individueller Urteile, anonymisierte Aggregation (AIJ), explizite Skalenkalibrierung und einen Red-Team-Durchgang adressiert, der Annahmen testweise infrage stellt.

Dokumentation und Nachvollziehbarkeit (ADR): Jede Gewichtungsrunde wird als ADR dokumentiert: Titel, Status, Datum, Teilnehmende, Methode (Swing/AHP), Rohdaten (Punktwerte/Matrix), Ergebnisvektor w , CR , Sensitivitätsergebnisse, Begründungen pro Kriterium, Gültigkeitsbereich, Review-Termin. ADRs werden signiert, versioniert und auf WORM-Speicher archiviert; die Score-Card referenziert die ADR-IDs.

Compliance, Schutzbedarf und Aufbewahrung: Evidenz und ADR-Artefakte werden klassifiziert, rollenbasiert zugänglich gemacht (RBAC) und über Signaturen/Chain-of-Custody geschützt. Aufbewahrungsfristen folgen Organisationsvorgaben (z. B. ≥ 24 Monate für AAR/Score-Cards).

Review-Zyklus, Revision und Trigger: Regelmäßiger Review mindestens halbjährlich. Revisions-Trigger: neue Föderationspartner/Standorte, veränderte Bedrohungslage, signifikante Last-/Skalierungsänderungen, neue regulatorische Vorgaben, Abweichungen in SLOs (Provisionierung/Reset/Orchestrierung) oder $CR \geq 0,10$. Bei Eintritt eines Triggers wird die Gewichtungsbildung erneut durchgeführt und als Nachtrags-ADR dokumentiert.

Eskalation und Konfliktlösung: Bei Dissens oder CR-Überschreitung erfolgt eine moderierte Zweitrunde mit Fokus auf widersprüchlichste Paare. Hält der Dissens an, entscheidet die Übungsleitung nach Konsultation von Security und Management; Abweichungen vom Standardprozess werden im ADR begründet.

Integration in Score-Card und Entscheidungsprozess: Freigegebene Gewichte werden in die Score-Card übernommen und für die Nutzwertanalyse verwendet. Sensitivitätsergebnisse und Szenario-Gewichte werden im Anhang referenziert, um den Entscheidungsweg vollständig nachvollziehbar zu halten.

Checkliste (Go/No-Go vor Veröffentlichung)

- CR unter Grenzwert (Standard $< 0,10$; bei $n \leq 3 < 0,05$) – geprüft und dokumentiert.
- Evidenzabdeckung ≥ 80 %; Quellen verlinkt und zugänglich.
- Bias-Kontrollen angewandt (Einzelurteile, Kalibrierung, Dokumentation starker Präferenzen).
- ADR erstellt, signiert, versioniert; Score-Card verweist auf ADR-ID.
- Sensitivitätsanalyse durchgeführt; Empfehlung robust gegen plausible Gewichtsspannen.
- Revisions-Trigger definiert; nächster Review-Termin gesetzt.

4.8 Schnittstellen- & Datenarchitektur

Dieses Kapitel spezifiziert (i) ein vollständiges Schnittstellen-Inventar der Trainingsplattform, (ii) Detailbeschreibungen der zentralen Schnittstellen (Zweck, Protokolle/Standards, Sicherheits- und Qualitätsmerkmale, Versionierung) sowie (iii) die Datenarchitektur mit Domänen- und Datenmodell, einschließlich Datenklassifizierung, Provenienz und einem kurzen, ausgefüllten Beispiel. Die Festlegungen gelten für beide Referenzarchitekturen; architekturspezifische Ausprägungen sind gekennzeichnet (A = VM-zentriert & HLA/DIS; B = Cloud-native/K8s & DDS/HLA-Bridge).

4.8.1 Schnittstellen-Übersicht

Dieses Inventar führt alle relevanten Schnittstellen der Trainingsplattform strukturiert und überprüfbar auf. Jede Zeile enthält ID, Name, Zweck, Technologie/Standard, Richtung/Zone, Authentisierung/Autorisierung (AuthN/Z), Versionierung und den Geltungsbereich in den Referenzarchitekturen (A, B).

Hinweis: Änderungen sind versioniert (SemVer bzw. Schema-IDs) umzusetzen. mTLS ist Mindeststandard; für Architektur B kommen Workload-Identitäten über SPIFFE/SPIRE (SVID) hinzu.

TABELLE 12 INTERFACE ÜBERSICHT

Kategorie	ID	Name	Zweck	Technologie/Standard	Richtung/Zone	AuthN/Z	Versionierung	Gilt für
Simulations-/Föderation	SI M-1	HLA Federation	Föderation von Simulationsobjekten/Interaktionen	IEEE 1516 (HLA), FOM/SOM	Föderations-VRF /Gateway	mTLS, kurzlebige Zertifikate	FOM-Version, Federation Agreement	A, B(Bridge)
Simulations-/Föderation	SI M-2	DIS Gateway	Gateway zu Live/Legacy-Geräten	IEEE 1278 (DIS)	Föderations-VRF /Gateway	mTLS, Export-Filter	PDU-Profile/Version	A, B(Bridge)
Simulations-/Föderation	SI M-3	DDS Domain/Topics	Pub/Sub-Datenbus für Sim-Events	OMG DDS	Übungs-/Mesh-Zone	mTLS (Mesh), SVID (SPIFFE)	Domain/Partition, QoS-Profile	B, A(Optional)
Simulations-/Föderation	SI M-4	DDS↔HLA Bridge	Mapping DDS-Topics ↔ HLA-Objekte	DDS+HLA	Föderations-Gateway	mTLS, Signaturen	Mapping-Schema (Version)	B (Kern), A(Optional)
Orchestrierung & Management	OR C-1	Orchestrierungs-API	Run-Lebenszyklus (Start/Pause/Stop, Eskalation)	gRPC/REST	Mgmt-Zone --> Übungs-Zone	mTLS, RBAC	SemVer (OpenAPI/Protos)	A, B
Orchestrierung & Management	OR C-2	Event-Injection	Einspielen von Events/Traffic	gRPC/REST, DDS/AMQP	Mgmt↔Übung	mTLS, Policy-Guards	Event-Schema-Version	A, B

Orchestrierung & Management	OR C-3	Szenario-Katalog	CRUD/Versionen von Szenarien	REST/gRPC, Git-Mirror (pull)	Mgmt	Signierte Tags/Merges	SemVer, Commit-Signaturen	A, B
Orchestrierung & Management	OR C-4	Parser/Validator	Schema/Syntax-Validierung (EaC)	REST/gRPC	Mgmt	mTLS	Schema-ID/Version	A, B
HIL & Realintegration	HIL-1	HIL-Adapter-API	Registrierung/Policy/Rate-Limits	REST/gRPC	Föderation/HIL-Zone	mTLS, Guards	Adapter-Profil-Version	A, B
HIL & Realintegration	HIL-2	Protokoll-Adapter	OT/ICS-Protokolle (OPC UA, Modbus, DNP3 etc.)	Gateway-spezifisch	HIL-Zone	mTLS, Whitelist	Profil-/Model-Version	A, B
Observability & AAR	OB S-1	Telemetrie-Ingest	Metriken/Logs/Traces/F lows ingestieren	OpenTelemetry (OTLP), Syslog, NetFlow/ I PFIX	Übung --> Observability	mTLS, write-controlled	Signal-Schema-Version	A, B
Observability & AAR	OB S-2	Monitoring-Abfragen	Dashboard s/Abfragen auf Observability-Daten	REST/Query-APIs	Mgmt --> Observability	RBAC, mTLS	API-SemVer	A, B
Observability & AAR	AA R-1	AAR-Export	Signiertes AAR-Paket (Timeline/Artefakte) exportieren	REST/S3-PUT, Offline-Export	Mgmt	Signaturen, Checksums	AAR-Manifest-Version	A, B
Observability & AAR	AA R-2	AAR-Import	Import externer/föderierter AARs	REST/S3-GET/Offline-Import	Mgmt	Signatur-/SBOM-Prüfung	Manifest-Version	A, B
Identität/Sicherheit/Polices	SE C-1	IdP/RBAC	AuthN/AuthZ (lokal, offline-fähig)	OIDC/SAML (lokal)	Mgmt & Portale	mTLS, Token TTL	Policy-/Role-Version	A, B
Identität/Sicherheit/Polices	SE C-2	PKI/CA	Zertifikatslebenszyklus, CRLs (offline)	X.509	Mgmt	Offline-CRLs	CA-Profil e/Version	A, B
Identität/Sicherheit/Polices	SE C-3	SPIFFE/SPIRE	Service-Identitäten (SVID)	SPIFFE/SPIRE	Mesh-Zone	mTLS	Trust Domain/Bundle-Version	B
Identität/Sicherheit/Polices	POL-1	Admission/Policy	Policies-as-Code, Admission	OPA/Gatekeeper, Kyverno	Mgmt --> Cluster	mTLS	Policy-Bundle-Version	B
Artefakt-/Supply-Chain	ART-1	Artefakt-Registry	Container/Charts/OVAs/Images bereitstellen	OCI Registry / OVA-Repository	Mgmt	Cosign-Sign., SBOM	Digest/Tag SemVer	A(OVA+Repo),

								B(O CI)
Artefakt- /Supply- Chain	ART-2	Git-Mirror	Szenario/LaC/Polices (pull)	Git (SSH/HTPS)	Mgmt	Signierte Commits/Tags	SemVer/Tags	A, B
Artefakt- /Supply- Chain	ART-3	Quarantäne-Service	Signatur/SBOM/AV-Prüfung	REST	Mgmt	mTLS	Prüfkatalog-Version	A, B
Zeit/Back up/Infrast ruktur	TIME-1	Zeitquelle	Zeitbasis für Stempel	NTP/GPS (lokal)	Alle Zonen	AuthN physisch	NTP-Stratum/Profil	A, B
Zeit/Back up/Infrast ruktur	BKP-1	Backup/Restore	etcd/Registry/AAR-Bacups	REST/CLI	Mgmt	Signaturen, WORM	Snapshot-Format-Version	A, B
Zeit/Back up/Infrast ruktur	STO-1	Objekt-Storage	AAR/Artefakt-Ablage	S3-kompatibel (lokal)	Mgmt/Ob servabilit y	mTLS, WORM	Bucket-Policy-Version	A, B
Portale & Lernsyst eme	POR-1	Lab-Portal-API	Labs/Resets/Guided Hints	REST	Übungs-Portale	RBAC/mTLS	API-SemVer	A, B
Portale & Lernsyst eme	SCORE-1	Scoring/Flags	Flag-Abnahme/Scoring-Events	REST/gRPC	Portal --> Scoring	mTLS	Event-Schema-Version	A, B
Portale & Lernsyst eme	LR-1	Lernstands-Export	Lernpfade/Badges exportieren	xAPI (optional) / CSV	Mgmt	mTLS/Signatur	Export-Schema-Version	A, B
Netz/Egr ess/Föde ration	FED-1	Föderations-Gateway	Site-to-Site (VRF/VPN)	IPsec/WireGuard + mTLS	Föderations-Zone	Keys rotieren	Föderations-Policy-Version	A, B
Netz/Egr ess/Föde ration	EGR-1	Egress-Proxy	Gated Outbound	HTTP(S)/TCP proxy	Mgmt/Ob serv.	mTLS, ACLs	Policy-Version	A, B

4.8.2 Schnittstellen Detailbeschreibungen

In diesem Kapitel werden die Schnittstellen präzisiert die im vorangegangenen Kapitel aufgeführt wurden. Für jede Kernschnittstelle werden Zweck und Einbettung, maßgebliche Standards und Protokolle, Datenmodell und Qualitätsmerkmale (QoS), Sicherheits- und Compliance-Anforderungen, Versionierung/Governance sowie Betriebs- und Testanforderungen spezifiziert. Der Bezug zu den Referenzarchitekturen A (VM-zentriert, HLA/DIS) und B (Cloud-native, DDS/Service-Mesh) wird hergestellt.

4.8.2.1 HLA-Föderation (SIM-1)

Zweck und Einbettung. Standardisierte Kopplung mehrerer Sites und Simulatoren zur koordinierten Durchführung föderierter Übungen. HLA dient als gemeinsame Sprache für Objektzustände und Interaktionen zwischen unabhängigen Simulations-Teilnehmern (Federates) und wird für Inter-Site-Sichten mit minimalem Datenaustausch eingesetzt.

Standard/Protokoll. IEEE 1516 (High Level Architecture, HLA). Artefaktgrundlage sind FOM/SOM-Spezifikationen (Federation/Object Models) sowie ein Federation Agreement mit Rollen, Zeitmanagement und Sicherheitsauflagen.

Transport und Zonen. Die Anbindung erfolgt über dedizierte Föderations-VRFs/VPNs. Alle Verbindungen sind mTLS-gesichert; Zertifikate sind kurzlebig und an Föderations-Runs gebunden. Join/Resign-Ereignisse werden vollständig protokolliert.

Datenmodell & QoS. Objektklassen und Interaktionen werden FOM-konform modelliert; Export-Sichten sind strikt minimal gehalten (Need-to-know). Optionales HLA-Zeitmanagement wird genutzt, wo Synchronität kritisch ist. Timeline-Drift wird gemessen und im AAR ausgewiesen.

Sicherheit & Compliance. Export-Filter durchsetzen Namensraum- und Attribut-Isolation. Federation-Keys rotieren pro Run; Audit-Trails sind unveränderlich (WORM). Policy-Verstöße führen zu Fail-Closed (Drop/Abbruch).

Versionierung & Governance. FOM-Version, Federation-ID und Run-ID sind Pflichtmetadaten. Änderungen an FOM/SOM erfolgen versioniert mit Kompatibilitätsmatrix; Major-Änderungen erfordern Migrationshinweise und Testnachweise.

Betriebs- und Testanforderungen. Pre-Flight-Tests (Handshake, Schema-Kompatibilität), 24-h-Disconnect-Probe ohne Datenverlust, Messung von Latenz/Drift, vollständige AAR-Evidenz.

Architekturbezug. Referenzarchitektur A: Kernbaustein. Referenzarchitektur B: Integration über DDS↔HLA-Bridge (SIM-4).

4.8.2.2 DDS-Domain/Topics (SIM-3) und DDS↔HLA-Bridge (SIM-4)

Zweck und Einbettung. Latenzarmer Pub/Sub-Bus für Simulations- und Trainingsereignisse mit feingranularen QoS-Profilen. Die Bridge koppelt DDS-Topics an HLA-Objekte/Interaktionen, um bestehende HLA-Ökosysteme einzubinden.

Standard/Protokoll. OMG DDS mit konfigurierbaren QoS-Parametern (Reliability, Durability, Deadline, Liveliness). Die Bridge implementiert ein beidseitiges Mapping von Topic-Schemas zu HLA-Attributen/Interaktionen.

Sicherheit & Identitäten. Transportverschlüsselung via mTLS; in Architektur B zusätzlich Workload-Identitäten über SPIFFE/SPIRE (SVID). Topic- und Partition-ACLs erzwingen Least Privilege; Telemetrie wird run-gebunden korreliert.

Datenmodell & QoS. Domains und Partitionen strukturieren die Datenflüsse (z. B. je Run/Site). QoS-Profile werden als Policies-as-Code versioniert; für HLA-Interop werden Framing und Semantik in der Bridge validiert.

Versionierung & Governance. Domain/Partition-IDs und Mapping-Schema sind semantisch versioniert. Änderungen durchlaufen Quarantäne→Staging→Produktion mit Kompatibilitätstests.

Betriebs- und Testanforderungen. Soak-Tests unter Last (P95-Latenz), Failover-Proben, Fuzzing des Mappings gegen Schema-Drift, AAR-Verknüpfung der QoS-Profile zur Reproduzierbarkeit.

Architekturbezug. Referenzarchitektur B: Kernbaustein (Service-Mesh gestützt). Referenzarchitektur A: optional via Bridge.

4.8.2.3 Orchestrierungs-API (ORC-1) und Event-Injection (ORC-2)

Zweck und Einbettung. Steuerung des Run-Lebenszyklus (Start, Stop, Pause, Eskalation), Ressourcenzuteilung und deterministisches Einspielen synthetischer Ereignisse/Traffic.



Spezifikation. OpenAPI/gRPC-Protos (SemVer) mit klaren Ressourcenmodellen (Run, ResourceQuota, Event). Kommandos sind idempotent; Fehlercodes/Retry-After sind definiert.

Sicherheit & Kontrolle. mTLS, rollenbasierte Autorisierung (Trainer:in/Übungsleitung), Audit-Pflicht für alle Zustandsübergänge; Policy-Guards verhindern unzulässige Aktionen.

Leistungsziele. Zustandsübergangs-Latenz < 5 s (P95); mindestens 10 parallele Runden ohne Ressourcenkonflikte.

Betriebs- und Testanforderungen. Pre-Flight-Checks (Signaturen, Quotas, Kompatibilität), deterministische Rollbacks bei Provisionierungsfehlern, Canary-Modus für neue Befehle.

Architekturbezug. Konsistent in A und B; in B zusätzlich durch Mesh-Policies (eBPF/NetworkPolicies) flankiert.

4.8.2.4 Szenario-Katalog und Parser (ORC-3/4)

Zweck und Einbettung. Versionierter Katalog mit Metadaten (Lernziele, Ressourcen, Sicherheitsstufe) und deklarativer Szenariobeschreibung (Topologie, Rollen, Events, Bewertungslogik).

Modell & Validierung. Everything-as-Code (YAML/JSON) mit Schema-IDs; Parser/Validator erzwingt syntaktische und semantische Korrektheit, verweist bei Fehlern auf Zeilen/Positionen und verhindert Freigabe bis zur Behebung.

Governance & Sicherheit. Vier-Augen-Freigabe, signierte Commits/Tags, Rollback-Fähigkeit. Hash/Signaturen aller Artefakte werden mitgeführt; sensible Vorlagen sind klassifiziert.

Betriebs- und Testanforderungen. Re-Provisionierung identischer Modelle $\geq 3 \times$ hash-identisch; Katalogaktionen auditierbar; Konformitätsprüfungen vor Promotion.

Architekturbezug. Gleichwertig für A und B; in B zusätzlich GITOps-Pull-Mechanik.

4.8.2.5 HIL-Adapter (HIL-1/2)

Zweck und Einbettung. Sichere, nachvollziehbare Anbindung realer Geräte (Hardware-in-the-Loop) ohne Verletzung der Isolationsgarantien des Übungsnetzes.

Sicherheit & Guards. Registrierung mit Policy/Rate-Limits, Whitelists und strikten Guards. Positiv-/Negativ-Tests vor Produktionsfreigabe; Ereignisse aus Realquellen werden eindeutig markiert.

Betriebskennzahlen. Kein Verkehr außerhalb definierter Guards; Latenzbudgets eingehalten; automatischer Fallback auf Emulation bei Störung oder Policy-Verstoß (sofortige Trennung + Alarm).

Architekturbezug. Pflichtfunktion in A (VM-Netze), in B über Gateways/Protokoll-Adapter und Mesh-Policies ergänzt.

4.8.2.6 Observability und AAR (OBS-1/2, AAR-1/2)

Ingest und Korrelation. Erfassung von Metriken, Logs, Traces und Netzflüssen via OTLP, Syslog und NetFlow/IPFIX. Korrelation run-gebunden über Run-ID und präzise Zeitstempel (lokale NTP/GPS-Quelle).

Abfragen und SLOs. Query-APIs und Dashboards mit Antwortzeiten < 2 s (P95) für Standard-Sichten; Export-Funktionen für didaktische Auswertungen.

AAR-Paket. Signiertes, reproduzierbares Paket (Manifest, Timeline, Artefakte, Prüfsummen, SBOM-Fingerprints) für deterministisches Replay kritischer Ereignisse.

Sicherheit & Betrieb. Write-controlled Observability-Zone, WORM-Ablage für AARs, Hash/Signatur-Verifikation im Export/Import; Zugriffe strikt RBAC-gesteuert.

Architekturbezug. Identisch nutzbar in A und B; in B Integration mit Mesh-Telemetrie/SVID-Attributen.

4.8.2.7 Identität und Policies (SEC-1/2/3, POL-1)

IdP/RBAC. Lokaler IdP (OIDC/SAML) mit Token-TTL und Offline-CRLs. Rollenmodell deckt Trainer:in/Übungsleitung, Teilnehmer:in und Beobachter:in ab; kritische Aktionen erfordern explizite Rechte.

PKI/CA. X.509-basierte Vertrauensanker; Rotation und Widerruf (CRLs) sind dokumentiert und offline-fähig. Föderations-Zertifikate sind kurzlebig und run-gebunden.

Workload-Identitäten (B). SPIFFE/SPIRE (SVID) für Zero-Trust-Policies im Service-Mesh; Admission-Kontrollen (OPA/Kyverno) sind fail-closed und über signierte Policy-Bundles versioniert.

Architekturbezug. Grundlegend für A und B; in B stärker automatisiert und feingranular durch Mesh/Admission.

4.8.2.8 Artefakt-/Supply-Chain (ART-1/2/3)

Registries und Repos. In A: OVA/VM-Image-Repository und Mirror; in B: lokale OCI-Registry für Container/Charts. Imports passieren eine Quarantäne-Stufe mit Signatur-, Hash- und SBOM-Prüfung sowie Offline-Scans.

Sicherheit & Provenienz. Cosign-Signaturen und SBOM-Pflicht für alle Artefakte; Promotion von Quarantäne über Staging nach Produktion nur bei bestandenen Funktions-/Sicherheits-Tests. Mirrors sind WORM-konfiguriert.

Governance & Versionierung. Signierte Commits/Tags, Vier-Augen-Merges, Digest-gebundene Promotion. Release-Notizen enthalten Hashes, SBOM-Fingerprints und Provenienz.

Architekturbezug. Gleichwertige Prozesse in A und B; in B zusätzlich GitOps-Pull-Synchronisation aus signiertem Git-Mirror.

4.8.3 Datenarchitektur

Dieses Kapitel beschreibt die Datenarchitektur der Trainingsplattform entlang eines konsistenten, auditierbaren und air-gap-fähigen Modells. Ziel ist eine eindeutige Korrelation sämtlicher Laufzeitergebnisse mit Szenarien und Runs, die Sicherstellung von Integrität und Provenienz aller Artefakte sowie die Durchsetzung von Mandantentrennung, Datenschutz und Reproduzierbarkeit. Die folgende Metamodell-Skizze (Abbildung 19 Metamodell der Datenarchitektur) ordnet die wesentlichen Domänenobjekte (Scenario, Run, Observability, AAR, Identitäten, Artefakte, Föderation) und ihre Beziehungen: Identifikatoren und Signaturen verknüpfen Datenflüsse deterministisch mit Run-Kontext, Zeitstempeln (lokale NTP/GPS-Quelle) und vertrauenswürdigen Quellen (PKI/SVID).

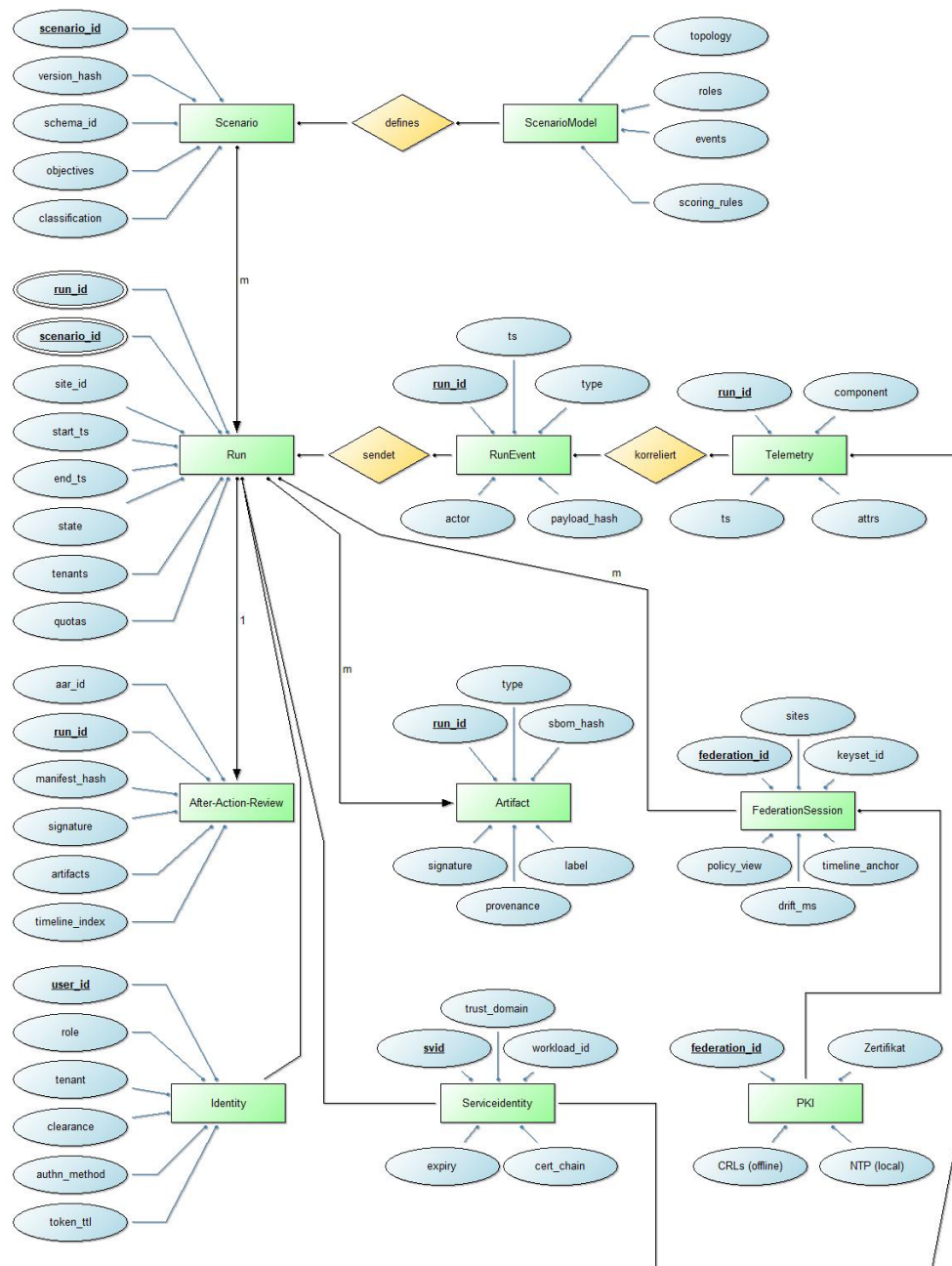


ABBILDUNG 19 METAMODELL DER DATENARCHITEKTUR

4.8.3.1 Identifikatoren, Versionierung & Provenienz

Zur eindeutigen Referenzierung werden Identifikatoren (etwa run_id, scenario_id, aar_id) kollisionsarm, über die gesamte Lebensdauer stabil und strikt maschinenlesbar gestaltet. Empfohlen wird ein wohldefiniertes Namensschema mit eingebetteten Kontextmerkmalen (z. B. Zeitstempel in UTC, Standortkürzel, Sequenznummer), sodass Eindeutigkeit und Sortierbarkeit zugleich gewährleistet sind. Jede auslieferbare Einheit (Artefakt) erhält einen kryptographischen Fingerabdruck auf Basis einer kollisionsresistenten Hashfunktion (mindestens SHA-256) sowie eine digitale Signatur; dadurch werden Integrität und Herkunft nachprüfbar. Ergänzend dokumentieren Software-Stücklisten (SBOM nach SPDX oder CycloneDX) und Build-Provenienz, wer, wann und mit welchen Eingaben bzw. Werkzeugversionen das Artefakt erzeugt hat. Änderungen folgen einem semantischen Versionsschema (SemVer) mit klarer Trennung von

inkompatiblen Hauptversionen (MAJOR), kompatiblen Erweiterungen (MINOR) und fehlerbehebenden Korrekturen (PATCH). Bevor ein Stand wirksam wird, erfolgt eine prüfbare Vier-Augen-Freigabe einschließlich Signaturprüfung und Policy-Checks; auf diese Weise bleiben Lieferkette und Genehmigungsweg nachvollziehbar. Sämtliche versions- und zustandsrelevanten Daten—einschließlich Release-Manifeste, Prüfsummen, Signaturen und Freigabeprotokolle—werden revisionssicher in Speicherbereichen mit WORM-Eigenschaft („Write Once, Read Many“) archiviert, um eine spätere Reproduktion und forensische Nachweisführung deterministisch zu ermöglichen.

4.8.3.2 Zeitbasis, Korrelation & Datenflüsse

Eine lokal betriebene, vertrauenswürdige Zeitquelle (NTP-Server der Stratum-1-Klasse mit GPS-Referenz; optional PTP für sub-Millisekunden-Genauigkeit) stellt konsistente, manipulationsresistente Zeitstempel bereit. Alle Ereignisse und Telemetriesignale führen die `run_id` als primären Korrelationsschlüssel sowie normierte Zeitangaben in UTC nach ISO-8601, wodurch eine eindeutige Zuordnung zu Szenario, Run und Föderationskontext möglich wird. Die Ingest-Pfade—OTLP für Metriken/Logs/Traces, Syslog für Systemereignisse, NetFlow/IPFIX für Netzwerkflüsse sowie DDS/HLA für Simulationsdaten—normalisieren je Quelle die Attributbezeichner und versehen jeden Datensatz mit einer Schema-Version (`schema_id`), einem Quellenmarker (`component`) und einem stabilen Inhaltsfingerabdruck (`payload_hash`) zur Duplikaterkennung und Integritätsprüfung. Zeitdrift zwischen Sites oder Subsystemen wird kontinuierlich gemessen, in den Metadaten vermerkt und im AAR transparent ausgewiesen; dadurch bleiben Reihenfolge und Kausalität von Ereignissen auch in föderierten oder temporär air-gapped Szenarien nachvollziehbar. Die Kombination aus präziser Zeitdisziplin, strengem Korrelationsschlüssel und kanonischer Attributnormalisierung erzeugt deterministische Evidenz für das After-Action-Review und ermöglicht performante Abfragen bei definierten SLOs (z. B. typische Dashboard-Queries im $P95 < 2\text{ s}$), ohne die Prüfbarkeit der Datenflüsse zu beeinträchtigen.

4.8.3.3 Standardobjekte

Die Run-Instanz bildet den administrativen Ablauf ab; die Telemetrie-Instanz korreliert über `run_id` und normierte Zeitstempel; das AAR-Manifest verweist über Hashes und Signaturen deterministisch auf Ereignisse und Artefakte, ohne hochschutzbedürftige Föderationsdetails einzubetten.

```
1  {
2    "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
3    "scenario_id": "SCN-2025-HTB-001",
4    "site_id": "AT-VIE",
5    "start_ts": "2025-11-18T09:00:00Z",
6    "end_ts": null,
7    "state": "running",
8    "tenants": ["Class-OFF-01"],
9    "quotas": {
10     "cpu_cores": 96,
11     "ram_gb": 384,
12     "storage_gb": 4000,
13     "net_mbps": 10000
14   }
15 }
```

ABBILDUNG 20 RUN-INSTANZ

Die Run-Instanz (Abbildung 20) beschreibt einen konkreten Übungsdurchlauf als administratives Aggregat. Der Identifikator `run_id` („RUN-2025-11-18-0900Z-AT-VIE-001“) ist kollisionsarm kodiert und enthält Datum und Startzeit in UTC, die Site-Kennung sowie eine Sequenznummer; er dient als primärer Korrelationsschlüssel für sämtliche Laufzeitdaten. `scenario_id` verweist auf die freigegebene Szenarioversion („SCN-2025-HTB-001“) und stellt damit den inhaltlichen Rahmen

her, während `site_id` („AT-VIE“) den physischen bzw. organisatorischen Ausführungsort eindeutig benennt. Die Felder `start_ts` und `end_ts` bilden die Zeitgrenzen in ISO-8601/UTC ab; solange der Durchlauf aktiv ist, bleibt `end_ts` null. Das Zustandsfeld `state` („running“) folgt einem wohldefinierten Zustandsautomaten (z. B. `planned` $\square$ `provisioning` $\square$ `running` $\square$ `paused` $\square$ `finished/aborted`) und ist Grundlage für Betriebsmetriken und SLO-Überwachung. Über `tenants` wird die Mandantenzuordnung („Class-OFF-01“) explizit gemacht; sie ermöglicht strikte Sichtbarkeitsgrenzen in Observability und AAR. Die Ressourcenvorgaben in `quotas` (CPU-Kerne, Arbeitsspeicher, Speicherplatz, Netzbudget) dienen der deterministischen Provisionierung, verhindern Noisy-Neighbor-Effekte und sind Bestandteil reproduzierbarer Plan/Apply-Pipelines.

```
1  {
2    "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
3    "ts": "2025-11-18T09:21:04.312Z",
4    "component": "netflow.collector",
5    "attrs": {
6      "src_ip": "10.60.12.45",
7      "src_port": 50432,
8      "dst_ip": "10.60.100.10",
9      "dst_port": 443,
10     "proto": "TCP",
11     "bytes": 18240,
12     "packets": 24,
13     "direction": "east-west",
14     "policy": "allow",
15     "sensor_id": "ATVIE-NF-01"
16   }
17 }
```

ABBILDUNG 21 TELEMETRIE-INSTANZ

Die Telemetrie-Instanz (Abbildung 21) ist run-gebunden und zeitlich normiert. Das Feld `run_id` stellt die eindeutige Zuordnung zum Durchlauf sicher; `ts` („2025-11-18T09:21:04.312Z“) liefert den präzisen UTC-Zeitstempel für Korrelation und spätere Replay-Fähigkeit. Mit `component` („netflow.collector“) wird die erzeugende Quelle benannt; dies erleichtert sowohl die Attributnormalisierung als auch die Fehlerlokalisierung. Der Nutzlastcontainer `attrs` hält die domänenspezifischen Messwerte in kanonischer Form: Quell- und Zieladressen/Ports (`src_ip`, `src_port`, `dst_ip`, `dst_port`), das verwendete Transportprotokoll (`proto`), Volumina (`bytes`, `packets`) sowie Kontextmerkmale wie Kommunikationsrichtung (`direction`), durchgesetzte Policy-Entscheidung (`policy`) und Sensoridentität (`sensor_id`). Diese Normalform ermöglicht es, heterogene Ingest-Pfade (z. B. NetFlow/IPFIX, Syslog, OTLP, DDS/HLA) in eine einheitliche, schema-versionierbare Repräsentation zu überführen, bei der jede Beobachtung deterministisch einem Run, einer Quelle und einem Zeitpunkt zugeordnet ist.

```

1  {
2    "aar_id": "AAR-2025-11-18-RUN-001",
3    "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
4    "manifest_hash": "sha256:6f7a7a2d1b2c0e2a4fda3be1c6c1b2d9ac77f0b7f2a0a2c44a7f8ea0459c9a10",
5    "signature": {
6      "algo": "ed25519",
7      "sig": "m1z1H0...c5Q=",
8      "signer": "aar-service@AT-VIE"
9    },
10   "artifacts": [
11     {
12       "type": "pcap",
13       "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
14       "sbom_hash": "sha256:aa17...ef91",
15       "signature": "MEQCIF5...==",
16       "label": "pcap-east-west-2025-11-18T09:05Z-09:35Z",
17       "provenance": "collector@ATVIE-NF-01"
18     },
19     {
20       "type": "report",
21       "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
22       "sbom_hash": "sha256:bb29...c013",
23       "signature": "MEVCIQw...==",
24       "label": "scoring-summary-v1",
25       "provenance": "scoring@ATVIE-SCORE-01"
26     },
27     {
28       "type": "screenshot",
29       "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
30       "sbom_hash": "sha256:cc34...ab77",
31       "signature": "MEUCIFH...==",
32       "label": "analyst-console-incident-42",
33       "provenance": "portal@ATVIE-LAB-PORTAL"
34     }
35   ],
36   "timeline_index": [
37     {
38       "ts": "2025-11-18T09:07:12.000Z",
39       "event_ref": {
40         "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
41         "type": "orchestration.start",

```

ABBILDUNG 22 AAR-MANIFEST PART 1

```

42     "payload_hash": "sha256:f1e0...109b"
43   },
44   "note": "Run gestartet (Standard-Range)."
45 },
46 {
47   "ts": "2025-11-18T09:21:04.312Z",
48   "event_ref": {
49     "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
50     "type": "scoring.flag.accepted",
51     "payload_hash": "sha256:9a5c...77e2"
52   },
53   "note": "Flag 42 akzeptiert; korreliert mit NetFlow-Peak."
54 },
55 {
56   "ts": "2025-11-18T09:31:45.900Z",
57   "event_ref": {
58     "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
59     "type": "orchestration.pause",
60     "payload_hash": "sha256:0c2b...fa64"
61   },
62   "note": "Kurze Pause; Eskalationsbesprechung."
63 },
64 {
65   "ts": "2025-11-18T09:52:10.102Z",
66   "event_ref": {
67     "run_id": "RUN-2025-11-18-0900Z-AT-VIE-001",
68     "type": "orchestration.finish",
69     "payload_hash": "sha256:7b23...c001"
70   },
71   "note": "Run abgeschlossen; AAR-Generierung initiiert."
72 }
73 ]
74 }

```

ABBILDUNG 23 AAR-MANIFEST PART 2



Das AAR-Manifest (Abbildung 22 und Abbildung 23) fungiert als signiertes, maschinenlesbares Inhaltsverzeichnis des Durchlaufs. `aar_id` identifiziert das Paket eindeutig und referenziert über `run_id` den zugrunde liegenden Run. Der Eintrag `manifest_hash` ist ein kryptografischer Fingerabdruck (SHA-256) des kanonisierten Manifests; er gewährleistet Integrität und erlaubt die unmittelbare Verifikation, dass Inhalt und Begleitdaten unverändert sind. Die Struktur `signature` spezifiziert Algorithmus, Signaturwert und Signierer („ed25519“, „aar-service@AT-VIE“) und macht die Provenienz des AAR nachvollziehbar. Unter `artifacts` sind die im Durchlauf erzeugten oder gebündelten Artefakte verzeichnet, jeweils mit Typ (z. B. `pcap`, `report`, `screenshot`), zugehöriger `run_id`, einem SBOM-Fingerabdruck (`sbom_hash`) und einer Artefakt-Signatur. Das Label unterstützt die menschliche Einordnung (z. B. ein Zeitfenster bei PCAPs), während `provenance` den erzeugenden Dienst dokumentiert (Collector, Scoring-Service, Portal). Der Abschnitt `timeline_index` bildet die didaktisch und betrieblich relevanten Schlüsselereignisse in zeitlicher Reihenfolge ab; jeder Eintrag enthält den UTC-Zeitpunkt, eine deterministische Referenz `event_ref` (mit `run_id`, `type` und einem `payload_hash` als stabiler Anker) sowie eine knappe Notiz zur Interpretation. Auf diese Weise lässt sich ein Replay kritischer Sequenzen exakt rekonstruieren, und die Prüfbarkeit (Chain-of-Custody) bleibt durchgängig gewahrt.

4.8.3.4 Beispiel: Föderierte Blue-Team-Übung „BLAU-ALP-01“

Rahmen: Zwei Sites (AT-VIE, Partner-Site), Air-Gap mit kontrolliertem Föderations-VRF. Szenario: Angriff auf Webapplikation, Detektion & Triage durch SOC-Team. Architektur: Referenz B (Kubernetes, Service-Mesh, DDS↔HLA-Bridge), AAR mit Replay.

1. Objektinventar und Primärklassifizierung
 - a. Szenariometadaten (Kurzbeschreibung, Lernziele, didaktische Hinweise ohne IP/Tool-Details): nicht klassifiziert (organisatorisch intern).
 - b. Szenariomodell (Topologie, IP-Räume, Rollen, Events, Scoring): EU RESTRICTED / EINGESCHRÄNKT (Offenlegung potenziell nachteilig).
 - c. Artefakte
 - a. Golden OVAs/Container-Images mit vorinstallierten Tools: EU RESTRICTED / EINGESCHRÄNKT (Supply-Chain-Risiko, aber keine hochsensitiven Inhalte).
 - b. Detektions-Regeln & Playbooks (TTP-spezifisch): EU CONFIDENTIAL / VERTRAULICH (Offenlegung schädlich).
 - d. Laufzeitdaten
 - a. Run-Events (Start/Stop/Pause, Eskalationen, Event-Injection): EU CONFIDENTIAL / VERTRAULICH.
 - b. Telemetrie-Schnitte (Metriken/Logs/Traces/Flows, korreliert via `run_id`): EU CONFIDENTIAL / VERTRAULICH.
 - e. Föderation
 - a. FederationSession-Material (Handshake-Protokolle, Mapping-Policies, kurzlebige Keys): EU SECRET / GEHEIM (Mindeststufe).
 - f. Vertrauensanker
 - a. CA-Private Keys, offline CRLs: EU SECRET / GEHEIM (bei weitreichender Systemwirkung ggf. TOP SECRET/STRENG GEHEIM).



- g. AAR-Paket (Manifest, Timeline, Replay-Index, ausgewählte Artefakte): durch Maximalprinzip → EU CONFIDENTIAL / VERTRAULICH.
2. Vererbungslogik (Maximalprinzip)
- a. Das AAR referenziert Telemetrie (EU C/AT Vertraulich) und Detektions-Regeln (EU C/AT Vertraulich). Obwohl einige Bestandteile nur „Restricted/Eingeschränkt“ sind, wird das AAR mindestens EU CONFIDENTIAL / VERTRAULICH, da die höchste enthaltene Stufe vererbt wird.
 - b. Die FederationSession bleibt eigenständig EU SECRET / GEHEIM und wird nicht in das AAR eingebettet, sondern nur über einen signierten Verweis (Proof of Federation) referenziert. So verhindert man, dass das AAR auf „Secret/Geheim“ hochgezogen würde.
3. Abgeleitete Kontrollen je Klasse (Auszug)
- a. EU CONFIDENTIAL / VERTRAULICH (AAR, Run-Events, Telemetrie-Schnitte): TLS 1.3/mTLS im Transport, Verschlüsselung at rest (AES-256), RBAC mit Run/Tenant-Scope, Signatur/Hash aller Exporte, WORM-Ablage des AAR (≥ 24 Monate), Quarantäne-Pfad für Export/Import (Signatur/SBOM-Prüfung), lückenlose Audit-Trails. EU SECRET / GEHEIM (CA-Keys, Federation-Keys): Offline-Tresor (HSM/TPM), Mehr-Augen-Prinzip, Offline-CRLs, strikt getrennte Admin-Pfade, kein direkter Bezug in AAR-Pakete, nur verifizierbare Referenz-Belege.

```
1
2
3 object: AAR
4 aar_id: AAR-2025-11-14-RUN-001
5 run_id: RUN-2025-11-14-0900Z-AT-VIE-001
6 classification:
7   eu: "CONFIDENTIEL UE / EU CONFIDENTIAL"
8   at: "VERTRAULICH"
9 owner: "Übungsleitung AT-VIE"
10 retention: "24m"
11 integrity:
12   package_hash: "sha256:..."
13   signature:
14     algo: "ed25519"
15     sig: "..."
16 provenance:
17   generated_by: "AAR-service@site-AT-VIE"
18   ts: "2025-11-14T11:07:12Z"
19 references:
20   - type: "telemetry.slice"
21     digest: "sha256:..."
22     classification:
23       eu: "CONFIDENTIEL UE / EU CONFIDENTIAL"
24       at: "VERTRAULICH"
25   - type: "detector.rules"
26     digest: "sha256:..."
27     classification:
28       eu: "CONFIDENTIEL UE / EU CONFIDENTIAL"
29       at: "VERTRAULICH"
```

ABBILDUNG 24 KLASSIFIZIERUNGSMETADATEN (BEISPIEL)

```
1 {  
2   "federation_proof": {  
3     "reference_only": true,  
4     "federation_id": "FED-2025-ALP-01",  
5     "handshake_digest": "sha256:...",  
6     "mapping_profile_id": "HLA-DDS-MAP-12",  
7     "drift_ms": 3,  
8     "signature": "ed25519:..."  
9   },  
10  "classification_note": "Proof stored at SECRET/GEHEIM; AAR remains CONFIDENTIAL/VERTRAULICH."  
11 }
```

ABBILDUNG 25 FÖDERATIONSNACHWEIS OHNE HOCHSTUFUNG DES AAR
(BEISPIEL)

4. Austausch mit EU-Organen (Äquivalenz)
 - a. Für das AAR werden die EUCI-Markierungen zweisprachig geführt („CONFIDENTIEL UE / EU CONFIDENTIAL“), das nationale Label „VERTRAULICH“ wird im Begleitvermerk zusätzlich angegeben. Die Federation-Belege verbleiben in der nationalen Geheimstufe und werden nur bei entsprechendem Bedarf und Kanal mit adäquater Schutzstufe ausgetauscht.
5. Lebenszyklus und Nachweis
 - a. Bei Create werden die Primärklassifizierungen gesetzt und in den Metadaten persistiert. In Use greift RBAC (und in Architektur B zusätzlich SVID) strikt rungebunden; Observability-Abfragen sind auditierbar. Beim Share/Federate sind Exportsichten minimal, Schlüssel kurzlebig und Pfade VRF/VPN-gekapselt; Driftmessungen fließen als Metrik in den AAR. Im Archive-Schritt wird das AAR signiert, auf WORM abgelegt und mit Hash/SBOM-Fingerprints referenzierbar archiviert. Das Dispose erfolgt nach Retention unter Berücksichtigung der Backups; Löschestätigungen werden journalisiert.

4.8.3.5 Schemas & Validierung

Die Datenobjekte der Plattform (insbesondere RunEvent, Telemetry und AAR-Manifest) werden durch formal spezifizierte Schemas beschrieben, die in JSON bzw. YAML vorliegen und als kanonische Verträge zwischen Erzeugern und Verbrauchern fungieren. Jedes Schema definiert Pflichtfelder (Mandatory Attributes), Datentypen (z. B. String, Integer, ISO-8601-Zeitstempel), Domänenrestriktionen (Wertebereiche, reguläre Ausdrücke, Enumerationen) sowie Referenzintegrität (z. B. die Existenz einer referenzierten run_id im Run-Katalog). Die Formalspezifikation ermöglicht deterministische Parser- und Validierungsroutinen, reduziert Interpretationsspielräume und bildet die Grundlage für maschinenlesbare Kompatibilitätsaussagen. Für JSON wird ein aktueller Draft der JSON-Schema-Spezifikation verwendet (mit klarer Angabe der Fassung), für API-Schnittstellen werden ergänzend OpenAPI/gRPC-Protos gepflegt; die verwendete Fassung ist in den Metadaten jedes Artefakts als schema_id referenziert.

Die Versionierung der Schemas folgt einem semantischen Muster (SemVer). MAJOR-Sprünge markieren bewusst inkompatible Änderungen (z. B. Umbenennung oder Entfernung von Pflichtfeldern), MINOR-Versionen erlauben additive, rückwärtskompatible Erweiterungen (z. B. neue optionale Felder), und PATCH-Versionen korrigieren Fehler ohne semantische Auswirkungen. Jede Datennutzlast trägt eine schema_id (Namensraum, Typklasse, Version) sowie



den Hash des Schemas, optional mit Signatur des Schema-Registrars; so ist im Nachhinein nachweisbar, gegen welchen Stand validiert wurde. Eine Kompatibilitätsmatrix hält fest, welche Verbraucher mit welchen Schema-Versionen interoperabel sind (Backward/Forward Compatibility), und bildet die Grundlage für kontrollierte Migrationen (z. B. Dual-Write/Dual-Read-Phasen, Deprecation-Fristen).

Die Validierung erfolgt mehrstufig und pipeline-integriert mit „fail-closed“-Semantik: Liegt kein positives Prüfergebnis vor, wird die Verarbeitung an der jeweiligen Stufe beendet. Erstens findet eine Entwicklungs- und Pre-Commit-Prüfung statt (Linting, statische Schema-Validierung, Property-Based-Tests auf Beispielpayloads). Zweitens wird in der CI/CD-Pipeline gegen den Schema-Katalog validiert; Policy-Checks (Policies-as-Code) prüfen zusätzlich nichtfunktionale Auflagen (z. B. maximale Feldlängen, Pflicht-Labels, Klassifizierungsmarken). Drittens wirkt an den Ingest-Gates der Laufzeit—also den Eintrittspunkten für OTLP/Syslog/NetFlow/IPFIX und DDS/HLA—eine transaktionale Validierung: Neben der Syntax/Typprüfung werden Referenzintegrität (existiert die `run_id`?), Zeitdisziplin (UTC/ISO-8601, Monotonie pro Quelle) und Kontextspezifika (z. B. erlaubte Werte für `component`) verifiziert. Viertens greift beim Export/Import (AAR-Erzeugung, AAR-Import aus Föderation) ein Quarantäne-Puffer: Pakete werden nur dann aus der Quarantäne in die Produktionsablage (WORM) überführt, wenn Schema-Konformität, Signaturen/Hashes und—falls gefordert—SBOM-Nachweise erfolgreich sind.

In allen Stufen gilt Fail-Closed: Nichtkonforme Datensätze werden blockiert, protokolliert und mit strukturierten Fehlermeldungen (Pfad zum Feld, erwarteter vs. beobachteter Typ/Wert, Schema-Version, Validator-Version) zurückgewiesen. Für Laufzeitpfade wird ein deterministischer Fehlercode (z. B. HTTP 422/UNPROCESSABLE_ENTITY für API-Ingest) und ein Retry-Protokoll mit Exponential Backoff empfohlen; dadurch bleibt das System robust gegenüber kurzzeitigen Inkonsistenzen, ohne die Beweisqualität zu kompromittieren. Nicht konforme Exporte/Importe verbleiben in der Quarantäne und werden weder indexiert noch in AAR-Pakete aufgenommen. Diese strikte Durchsetzung ist insbesondere in air-gapped Umgebungen bedeutsam, weil hier die Validierung die Rolle des letzten technischen Gatekeepers übernimmt.

Über die reine Schema-Konformität hinaus werden semantische Invarianten geprüft. Beispiele sind Eindeutigkeit (keine Doppelverwendung derselben `aar_id`), Plausibilität (Zeitfenster im AAR müssen innerhalb der Run-Dauer liegen), Kohärenz (ein `timeline_index`-Eintrag muss auf ein existierendes RunEvent mit identischem `payload_hash` verweisen) und Klassifizierungskohärenz (aus den referenzierten Objekten abgeleitete Schutzstufe $\geq$ deklariertem Label; Maximalprinzip). Diese Prüfungen werden als regelbasierte Validatoren implementiert und in eine Policy-Engine eingebunden; der verwendete Policy-Stand wird (ähnlich dem Schema) gehasht, signiert und im AAR-Manifest als Validierungsnachweis abgelegt.

Die Laufzeitmechanik ist damit transparent: Ein eingehender Telemetriedatensatz passiert zunächst die Syntax-/Typprüfung (gegen die `schema_id`), anschließend Kontext- und Referenzprüfungen (Existenz von `run_id`, Zeitbasis, zulässige `component`-Werte) und schließlich Policy-Kontrollen (z. B. Feldmaskierung für personenbezogene Attribute). Nur bei Erfolg wird der Datensatz persistiert und für Korrelation/Abfragen freigegeben. Vor der AAR-Erzeugung aggregiert ein AAR-Builder die relevanten RunEvents, Telemetrie-Slices und Artefakte, überprüft erneut Kohärenz und Integrität (Hashes/Signaturen), erzeugt einen `manifest_hash`, signiert das Manifest und schreibt einen kompakten Validierungsreport (Schema-IDs, Validator-Versionen, Policy-Bundle-Hash, Zeit der Prüfung) in die Metadaten. Beim AAR-Import wird derselbe Prüffächer erneut durchlaufen; Importpfade sind auf read-only gesetzt und können die Produktion nicht verändern, solange die Validierung nicht erfolgreich ist.

Zur Governance gehören ein kontrollierter Schema-Katalog (Registry) mit Namensräumen pro Domäne (z. B. `telemetry.netflow.v1.2.0`, `orchestration.event.v2.1.0`, `aar.manifest.v1.0.3`),

dokumentierte Änderungsprozesse (RFC/ADR, Review, Vier-Augen-Freigabe), Deprecation-Richtlinien (Ankündigungsfristen, Parallelbetrieb), sowie periodische Konformitätstests (Golden Samples, Property-Based-Fuzzing, Re-Validation historischer AAR-Pakete). Für föderierte Szenarien werden Mapping-Validatoren betrieben, die DDS/HLA-Sichten gegen die lokalen Schemas prüfen und Drift/Verluste (Schema- oder QoS-bedingt) quantifizieren; die Ergebnisse fließen als Evidenz in das AAR (z. B. als validation.report-Verweis) ein.

Schließlich sind Betriebskennzahlen definiert, um die Wirksamkeit der Validierung messbar zu machen: typische Validierungslatenz pro Datensatz (Ziel im niedrigen Millisekundenbereich für Online-Ingest), Durchsatz (Ereignisse/s pro Ingest-Kanal), Fehlerrate nach Kategorien (Syntax, Referenz, Policy), sowie Zeit bis zur AAR-Freigabe nach erfolgreicher Prüfung. Diese Metriken werden im Observability-Stack erfasst und als betriebliches SLO überwacht. Zusammen gewährleisten die formalen Schemas, die strenge, mehrstufige Validierung und die dokumentierte Governance eine reproduzierbare, auditfeste und interoperable Datenbasis—eine notwendige Voraussetzung für deterministisches Replay, belastbare After-Action-Analysen und den sicheren Betrieb in offline- bzw. föderationsfähigen Trainingsumgebungen.

4.8.3.6 Föderationsdaten & Austauschprofile

Föderation bezeichnet den geregelten, temporären Zusammenschluss mehrerer, voneinander souveräner Trainingsumgebungen zu einer gemeinsamen Übung. Die dafür erforderlichen Daten und Nachweise werden als Föderationsdaten (z. B. Handshake-Evidenzen, Mapping-Profile, Qualitäts- und Drift-Metriken) in einer höheren Schutzstufe außerhalb des AAR geführt und im AAR ausschließlich referenziert. Dieses Trennprinzip verhindert, dass das AAR aufgrund eingebetteter Geheimnisse hochgestuft werden muss, und erhält zugleich die volle Prüfbarkeit über kryptographisch gesicherte Verweise (Digest/Signatur).

Zweck und Umfang der Föderationsdaten. Kernelemente sind (i) Handshake-Belege (Wer hat wann mit welchen Schlüsseln und Parametern die Föderation aufgebaut?), (ii) Austauschprofile („Mapping-Profile“), die festlegen, welche Klassen/Felder/Topics unter welchen QoS-Bedingungen ausgetauscht werden, sowie (iii) Metriken zur Zeit- und Qualitätskohärenz (insb. Timeline-Drift, Verlust- bzw. Mapping-Fehlerquoten). Diese Artefakte bilden den nachweisbaren Vertrag zwischen den Sites: Sie dokumentieren den Umfang der Exportsicht (Minimalprinzip, Feld- und Objekt-Whitelist), die Sicherheitsparameter (mTLS-Profile, Schlüssellebensdauer, Revokation), die Interoperabilitätsregeln (z. B. DDS-QoS, HLA-FOM-Sichten) und die Prüfkriterien für einen geordneten Betrieb (z. B. maximal tolerierte Drift).

Schutzbedarf und Ablage. Föderationsdaten werden in einer dedizierten, stärker geschützten Ablage („Federation Vault“) geführt. Schlüsselmaterial, CRLs, Mapping-Profile und Handshake-Logs sind signiert, versioniert und WORM-fähig archiviert; Zugriffe erfolgen über fein-granulares RBAC bzw. Workload-Identitäten (SPIFFE/SVID in der Kubernetes-Variante) mit Vier-Augen-Freigabe für sensible Operationen (z. B. Key-Rotation, Profil-Änderung). Das AAR enthält lediglich einen „proof-of-federation“ (z. B. federation_id, Hash/Signatur der Vereinbarung, Profil-Version, Drift-Statistik) und kann dadurch vertraulich bleiben, obwohl die zugrunde liegenden Belege geheim sind.

Austauschprofile (Mapping-Profile). Das Austauschprofil legt die Exportsicht präzise fest: zulässige Objekt-/Feldmengen (HLA-FOM-Sicht bzw. DDS-Topic/Type-Subset), Normalisierung/Reduktion (Feldmaskierung, Pseudonymisierung), Qualitätsanforderungen (DDS-Reliability/Durability, HLA-Zeitmanagement-Vorgaben), Namensraum- und Rollenbezüge (Mandant/Run-Scope) sowie Kompatibilitätsaussagen (Schema-Versionen, zulässige Minor-Upgrades). Profile sind semantisch versioniert; MAJOR-Sprünge gelten als inkompatibel und erfordern explizite Re-Freigabe. Jede

laufende Föderation bindet die konkrete Profilversion und ihre Signatur als Referenz, sodass im Streitfall eindeutig ist, welche Sichten freigegeben waren.

Identität, Schlüssel und Transport. Föderationsstrecken werden ausschließlich über dedizierte VRF/VPN-Segmente betrieben. Die beiderseitige Authentisierung erfolgt via mTLS mit kurzlebigen, kontextgebundenen Schlüsseln/Zertifikaten (z. B. pro Session/Run), die aus einer vertrauenswürdigen PKI abgeleitet und mit Offline-CRLs/OCSP-Ersatz betriebssicher widerrufen werden können. In Cloud-nativen Umgebungen werden zusätzlich Service-Identitäten (SVID) an den Gateways durchgesetzt, um Zero-Trust-Policies bis auf Workload-Ebene durchzuhalten. Schlüsselrotation und Session-Beendigung sind transaktional: Beim Rollover wird die neue Kette voraktiviert und nach erfolgreichem Handshake atomar übernommen; bei Abbruch wird die Strecke fail-closed getrennt und im Vault protokolliert.

Zeitbasis und Drift-Kontrolle. Föderierte Runs erfordern eine gemeinsame Zeitdisziplin (lokale NTP/GPS/PTP-Quelle je Site, definierte Stratum- und Jitter-Budgets). Während der Übung werden Drift-Metriken fortlaufend gemessen und als Evidenzwerte (z. B. P50/P95-Drift in Millisekunden, Anzahl Korrektur-Events) im Föderationsbereich erfasst. Das AAR referenziert diese Metriken (Proof-Verweis) und weist u. a. „Drift in ms“ sowie ggf. ein Unsicherheitsintervall für Replay-Analysen aus. Überschreitet die Drift definierte Grenzwerte, greifen Abhilferegeln (Resync, Rate-Limit, Degradationsmodus) oder ein kontrolliertes Unfencing der Strecke.

Gating und Validierung. Der Föderationsaufbau unterliegt Gating-Bedingungen: Schema- und QoS-Kompatibilität der Mapping-Profile, erfolgreiche Schlüsselprüfung, VRF/VPN-Erreichbarkeit, Zeitbasistests sowie Negativtests (z. B. keine verbotenen Objekte in der Exportsicht). Das Ergebnis wird als Handshake-Evidenz (Hashes, Signaturen, Testergebnisse) abgelegt. Während der Laufzeit wirken Policy-Guards (z. B. Feld- und Objekt-Filter, Rate-Limits, DLP-Regeln) am Gateway. Nicht konforme Nachrichten werden fail-closed verworfen und mit strukturierten Fehlercodes protokolliert; Schwellen-verletzungen lösen Alarmierung und—je nach Kritikalität—automatische Entkopplung aus.

Fehlerbehandlung und Abschluss. Fehlerfälle (z. B. Zertifikatsfehler, Profil-Drift, QoS-Inkonsistenz) führen zu definierten Eskalationspfaden: Quarantäne des betroffenen Flusses, forciertes Key-Rollover, temporäre Read-Only-Degradation oder harte Trennung der Strecke. Die Beendigungsprozedur widerruft alle kurzlebigen Schlüssel, friert die Profilversion ein, schreibt einen Abschluss-Report (Statistiken, Verstöße, Drifts, Ausfallzeiten) und stellt die Evidenzen revisionssicher im Vault ein. Das AAR erhält nur den signierten Proof-Block (ID, Profil-Version, Metrik-Zusammenfassung, Hash/Signatur-Verweise) und bleibt damit schlank und klassifikationsarm.

Betriebs- und Governance-Aspekte. Ein Federation-Katalog hält zulässige Partner, genehmigte Profile, Schlüssel- und Vertrauensbeziehungen sowie Deprecation-Fristen vor. Änderungen durchlaufen ADR/RFC-Prozesse mit Vier-Augen-Freigabe und Test-Nachweis (Interoperabilität, Last- und Drift-Szenarien). Betriebskennzahlen umfassen u. a. Handshake-Erfolgsquote, Zeit bis Föderationsbereitschaft, Durchsatz/Latenz auf der Föderationsstrecke, Drift-Statistiken und Policy-Verstoßraten. Diese Metriken sind Teil der Observability und werden gegen SLOs überwacht.

4.8.3.7 Datenklassifizierung und Schutzbedarf

Die vorliegende Datenklassifizierung für die Trainingsplattform orientiert sich an den Stufen des EU-Klassifizierungssystems (EU Classified Information, EUCI) sowie an den österreichischen Vorgaben nach InfOG und den zugehörigen Verordnungen. Ziel ist eine risikobasierte, reproduzierbare und air-gap-taugliche Ableitung technischer und organisatorischer Kontrollen über den gesamten Lebenszyklus von Informationen und Artefakten – von der Szenarioerstellung über Provisionierung und Laufzeitbetrieb bis hin zu After-Action-Review, Archivierung und Löschung.



Grundlage der Einstufung ist das Schadenausmaß, das eine Offenlegung, Manipulation oder Nichtverfügbarkeit von Informationen nach sich ziehen würde. Für EUCI wird zwischen EU TOP SECRET beziehungsweise TRÈS SECRET UE, EU SECRET beziehungsweise SECRET UE, EU CONFIDENTIAL beziehungsweise CONFIDENTIEL UE und EU RESTRICTED beziehungsweise RESTREINT UE differenziert; national werden die Stufen STRENG GEHEIM, GEHEIM, VERTRAULICH und EINGESCHRÄNKT herangezogen, wobei nicht klassifizierte Inhalte als nicht-öffentlich zu behandeln sind. Markierungen erfolgen konform zu den jeweiligen Systemen, also zweisprachig für EUCI und in Majuskeln für österreichische Stufen.

Die praxisüblichen Arbeitsklassen „Öffentlich“, „Intern“, „Vertraulich“ und „Streng vertraulich“ lassen sich konsistent in diese Systeme überführen. Inhalte ohne Schutzbedarf bleiben unklassifiziert, werden jedoch hinsichtlich Integrität sinnvollerweise mit Basiskontrollen versehen. „Intern“ wird dann unklassifiziert geführt, wenn keine nachteiligen Folgen einer Offenlegung zu erwarten sind; sobald ein nachteiliger Effekt möglich erscheint, ist mindestens EU RESTRICTED beziehungsweise EINGESCHRÄNKT zu wählen. Materialien, deren Verlust oder Offenlegung voraussichtlich schädliche Auswirkungen auf Betrieb, Übungen oder Partner hätte – etwa Szenarioartefakte, Run-Daten, AAR-Pakete oder Identitätsinformationen –, sind als EU CONFIDENTIAL beziehungsweise VERTRAULICH zu behandeln. Vertrauensanker wie CA-Private-Keys, Föderations-Keysets oder offline geführte CRL-Artefakte begründen regelmäßig EU SECRET beziehungsweise GEHEIM, und nur bei plausibel drohendem äußerst schwerem Schaden ist die Einstufung bis EU TOP SECRET beziehungsweise STRENG GEHEIM anzuheben. EUCI ist für EU-Informationen maßgeblich, während für rein nationale Inhalte die österreichischen Stufen zur Anwendung kommen; bei grenzüberschreitendem Austausch ist die Äquivalenz der Markierungen explizit zu kennzeichnen.

Die Klassifizierung wird objektscharf vergeben und entlang von Referenzen vererbt. Für zusammengesetzte Informationsobjekte gilt ein Maximalprinzip: Die effektive Klassifizierung entspricht der höchsten Stufe unter allen eingebetteten oder referenzierten Bestandteilen. Ein AAR-Paket, das vertrauliche Run-Artefakte enthält, ist damit mindestens vertraulich im nationalen Sinn bzw. EU-confidential. Eine Herabstufung abgeleiteter Daten – etwa durch Aggregation oder Pseudonymisierung – ist nur zulässig, wenn die Verfahren dokumentiert sind, die Rückführbarkeit auf Einzelpersonen oder sensible Konfigurationen technisch ausgeschlossen ist und eine formale Freigabe vorliegt. Unklare oder unvollständig bewertete Objekte werden bis zum Abschluss der Analyse konservativ als vertraulich geführt. Die Klassifizierungsmetadaten sind maschinenlesbar zu erfassen und umfassen neben der Stufe den oder die Eigentümer, Retentionsfristen, Referenzen, Integritäts- und Signaturnachweise sowie Provenienzanangaben.

Aus der Stufe werden Basiskontrollen abgeleitet, die sowohl den Transport als auch die Speicherung und den Zugriff regeln. Für unklassifizierte und interne Inhalte genügen transportseitig zeitgemäße Protokolle, wohingegen für EU-restricted beziehungsweise eingeschränkte Informationen mTLS verpflichtend wird und Zugriffe zu protokollieren sind. Vertrauliche beziehungsweise EU-confidential Daten sind in Transit und at Rest mit starken Verfahren abzusichern; hierzu zählen TLS 1.3 mit beiderseitiger Authentisierung, ruhende Verschlüsselung mit dokumentierter Schlüsselrotation, durchgängige Signatur- und Hash-Nachweise sowie die strikte Durchsetzung von Least-Privilege und kontextgebundenen Geltungsbereichen nach Run und Mandant. Für geheime und streng geheime Informationen sind zusätzlich workload-gebundene Identitäten – in der Kubernetes-Variante etwa SPIFFE/SVID – sowie HSM- oder TPM-gestützte Schlüsselverwaltung und offline geführte Sperrlisten vorzusehen; administrative Pfade sind physisch oder logisch zu trennen und durch Mehr-Augen-Prinzipien zu sichern. In Bezug auf Speicherung und Aufbewahrung sind AAR-Pakete für vertrauliche Einstufungen auf WORM-fähige Speicherbereiche abzulegen und mit signierten Manifesten zu versehen; Schlüsselmaterial auf höheren Stufen verbleibt im Offline-Tresor mit dokumentierter Rotation, Widerruf und Nachweis der

Zugriffskette. Föderierte Übermittlungen erfolgen ausschließlich über dedizierte, gekapselte Transportpfade mit kurzlebigen Schlüsseln und minimalen Exportsichten; Handshakes, Mappings und mögliche Zeitdrifts sind zu protokollieren und in den AAR-Evidenzen auszuweisen. Die Wirksamkeit der Kontrollen ist regelmäßig anhand von Disconnect-Proben, Wiederherstellungstests gegen definierte RTO/RPO-Ziele und automatisierten Policy-Prüfungen zu evaluieren und in Architekturentscheidungen sowie After-Action-Reports zu dokumentieren.

Der Lebenszyklus folgt einem konsistenten Muster. Bei der Erzeugung werden Primärklassifizierung, Eigentum, Retention und Schutzbedarf in Metadaten festgehalten, und sämtliche Artefakte erhalten Integritäts- und Provenienznachweise. In der Nutzung sind Zugriffe strikt rollenbasiert und – sofern die Cloud-native-Architektur eingesetzt wird – zusätzlich über workload-gebundene Identitäten an den jeweiligen Run- und Tenant-Kontext gebunden; Audit-Trails sind lückenlos zu führen. Beim Austausch, insbesondere in föderierten Übungen, sind Exportsichten auf das erforderliche Minimum zu begrenzen und über kurzlebige Schlüssel in dedizierten VRF/VPN-Strecken abzusichern; Driftmessungen und Mapping-Policies sind Teil der Betriebsdokumentation. In der Archivphase werden AAR-Pakete klassenkonform und revisionssicher aufbewahrt; Signatur- und Hash-Werte, SBOM-Fingerabdrücke und Versionsinformationen bleiben dauerhaft referenzierbar. Das Löschen erfolgt nach Ablauf der Retention unter Verifikation und unter Einbezug von Sicherungskopien; Ausnahmen im Rahmen rechtlicher Vorhalte sind nachvollziehbar zu begründen.

Die Anwendung dieser Regeln auf typische Objekttypen des Trainingsbetriebs verdeutlicht das Vorgehen. Szenariometadaten wie Kurzbeschreibungen und Lernziele bleiben im Regelfall unklassifiziert und organisatorisch intern; enthalten sie jedoch operative Details wie IP-Räume, spezifische Werkzeuge oder TTP-Profile, ist mindestens EU-restricted beziehungsweise eingeschränkt zu vergeben. AAR-Pakete einschließlich Timelines, Replay-Indizes und Artefaktbezügen sind vertraulich zu behandeln und mit Signaturen, Hash-Werten und WORM-Ablage zu sichern; Import und Export haben in air-gap-fähigen Quarantänepfaden mit Signatur- und SBOM-Prüfungen zu erfolgen. Laufzeitdaten und Telemetrieausschnitte, die über Run-IDs korreliert sind, werden in der Regel vertraulich geführt; eine Absenkung setzt eine dokumentierte, irreversible Anonymisierung oder Aggregation voraus. Für Vertrauensanker wie Föderations-Schlüsselbündel, CA-Schlüssel und offline verwaltete CRLs ist mindestens die geheime Stufe vorzusehen; bei besonders weitreichenden Integritäts- oder Souveränitätsrisiken ist die streng geheime Stufe zu prüfen. In allen Fällen gilt, dass bei internationalem Austausch die Äquivalenz der Kennzeichnungen zwischen EUCI und den österreichischen Stufen explizit herzustellen ist, damit die empfangenden Stellen die Informationen korrekt behandeln können.

Mit dieser Klassifikationslogik wird die inhaltliche Schutzbedarfsanalyse konsistent auf technische und organisatorische Maßnahmen abgebildet. Sie ermöglicht nachprüfbare Compliance im air-gapped Betrieb, stützt die Reproduzierbarkeit und Forensik über signierte Evidenzen und schafft robuste Leitplanken für föderierte Übungen, in denen Sicherheitsinteressen und Interoperabilität zugleich gewahrt bleiben.

4.9 Sicherheit & Compliance

Ziel dieses Kapitels ist ein konsistentes Sicherheits- und Compliance-Rahmenwerk für den Trainingsbetrieb unter Offline-/Air-Gap-Bedingungen und in föderierten Übungen. Die Gestaltung folgt den Prinzipien „least privilege“, „defense in depth“, „controls-as-code“ und Nachweisfähigkeit (prüfbare Evidenz). Sicherheitsfunktionen sind deterministisch testbar, policy-gesteuert und technisch erzwungen; alle Schlüsselfunktionen (Identität, Schlüsselmaterial, Zeitquelle, Protokollierung) sind offline funktionsfähig.

4.9.1 Zonen- und Segmentierungsmodell

Die Sicherheitsarchitektur der Trainingsplattform folgt einem mehrschichtigen Zonenmodell, das logische und physische Trennungen systematisch kombiniert, um Angriffsflächen zu minimieren, Nachweisfähigkeit zu erhöhen und Air-Gap-Betrieb reproduzierbar zu machen. Zonen definieren wohlfundierte Vertrauensdomänen mit klar zugeordneten Assets, Identitätsmodellen, Protokollprofilen und Durchleitungsregeln. Segmentierung wird in Referenzarchitektur A primär über Hypervisor-, VLAN- und VRF-Mechanismen durchgesetzt, während Referenzarchitektur B diese Grundtrennung zusätzlich mit Namespace-Isolation, Kubernetes-NetworkPolicies sowie Service-Mesh-Policies und mTLS-by-default auf der Workload-Ebene verfeinert. In beiden Varianten gilt das Prinzip „default deny“: Ohne explizite Freigabe existiert keine Erreichbarkeit zwischen Zonen.

Das Zonenmodell (Abbildung 26) umfasst fünf Zonen. Die (1) Management-Zone beherbergt die Steuerungs- und Vertrauen-Dienste einschließlich Orchestrierung, Szenariokatalog und Parser, lokales Identitäts- und Berechtigungssystem (IdP/PKI), AAR-Service sowie die Artefakt-Quarantäne. Der Zugriff erfolgt ausschließlich über gehärtete Jump-Hosts mit starker Authentisierung; sämtliche Schnittstellen werden über mTLS und rollenbasierte Zugriffskontrollen abgesichert und revisionssicher protokolliert. Die (2) Übungs-/Trainings-Zone enthält die Szenario-Workloads—als virtuelle Maschinen in A oder Pods in B—sowie didaktische Frontends wie Hands-on-Portale und Scoring-Dienste. Innerhalb dieser Zone sind Kommunikationsbeziehungen strikt policy-basiert freizugeben, und Ressourcenquoten (z. B. CPU, RAM, Storage und Netz) verhindern Noisy-Neighbor-Effekte und sichern die Reproduzierbarkeit von Bereitstellungszeiten. Die (3) Observability-Zone aggregiert Mess- und Ereignisdaten über normierte Ingest-Pfade (z. B. OTLP für Metriken/Logs/Traces, Syslog für Systemereignisse, NetFlow/IPFIX für Flüsse) und bietet korrelierte Sichten und Dashboards. Sie ist als „write-controlled“ ausgelegt, das heißt, es existiert kein direkter Rückkanal in Übungs-Workloads; Anfragen aus der Management-Zone sind ausschließlich lesend und RBAC-geschützt. Die Föderations-Zone (4) stellt dedizierte Gateways und Brücken zur Kopplung mit Partner-Sites bereit—in A primär HLA/DIS, in B DDS-Domänen mit HLA-Bridge—und nutzt zur Transportkapselung eigens reservierte VRF/VPN-Strecken mit kurzlebigen, kontextgebundenen Schlüsseln. Die HIL-/Real-Integrations-Zone (5) führt Adapter und Proxies zur kontrollierten Einbindung realer Geräte; sie wird durch Guards, Richtlinien und Rate-Limits technisch abgesichert, und alle Ereignisse aus realen Quellen sind eindeutig markiert.



ABBILDUNG 26 ZONENMODELL

Die Durchleitungsregeln zwischen Zonen sind minimalistisch und streng gerichtet. Steuerungsbefehle fließen ausschließlich von der Management-Zone in die Übungs-Zone über wohldefinierte Orchestrierungs-APIs; Observability nimmt Schreibzugriffe nur aus Übungs- und Föderations-Zonen entgegen und beantwortet Leseanfragen ausschließlich in Richtung Management. Föderationsverkehr ist vollständig von regulären Übungsflüssen entkoppelt und verläuft nur über die Föderations-VRFs, die ihrerseits mTLS, kurzlebige Zertifikate und standardisierte Austauschprofile erzwingen. Realgeräte-Ereignisse treten ausschließlich über die HIL-Zone ein; negative Tests und Rate-Limits sind operative Vorbedingungen, und Verstöße führen fail-closed zur sofortigen Trennung. In Referenzarchitektur B werden diese Regeln zusätzlich auf Workload-Ebene gespiegelt: NetworkPolicies beschränken Pod-zu-Pod-Verbindungen innerhalb von Namespaces, während das Service-Mesh Ende-zu-Ende-Identitäten (SPIFFE/SVID) durchsetzt und damit Zero-Trust-Policies bis auf Dienstebene ermöglicht. In Referenzarchitektur A werden die korrespondierenden Kontrollen über VRF/VLAN-Isolierung, Host-Firewalls und Gateways abgebildet; Identitäten werden als X.509-Dienstzertifikate geführt.

Der Air-Gap-Betrieb ist als Standardzustand definiert. Die Plattform arbeitet vollständig offline, das heißt ohne Abhängigkeiten von externen Namensdiensten, Update-Quellen oder Validierungsendpunkten. Kurzzeitige, streng gesicherte Egress-Fenster—beispielsweise zur Synchronisation der Zeitbasis oder zur Aktualisierung offline gespiegelt vorgehaltener Sperrlisten—werden technisch „gated“, kryptografisch authentisiert, lückenlos protokolliert und durch formale Freigabeprozesse begrenzt. Ein periodischer Disconnect-Test über mindestens 24 Stunden dient als Wirksamkeitsnachweis: Während dieser Zeit müssen alle Kernfunktionen, einschließlich Provisionierung, Orchestrierung, Observability und AAR-Erzeugung, ohne externe Verbindungen vollständig verfügbar bleiben; die Protokolle dürfen keine externen Kontaktversuche ausweisen. Für föderierte Übungen werden ausschließlich die Föderations-VRFs temporär aktiviert; ihre Aktivierung und Deaktivierung, Schlüsselrotation sowie Handshake-Evidenzen werden als hochschutzbedürftige Belege in einer sicheren Ablage („Federation Vault“) versioniert.

Die Segmentierungsmechanismen werden als „controls-as-code“ betrieben und damit test- und auditfähig. In A sind VRF- und VLAN-Zuweisungen, Gateway-Regeln und Host-Firewalls als deklarative Konfigurationen versioniert; in B werden zusätzlich Admission-Policies (z. B. OPA/Gatekeeper oder Kyverno), NetworkPolicies und Mesh-Intent (mTLS-Profil, Autorisierungsregeln, Traffic-Shaping) semantisch versioniert und signiert. Änderungen passieren Vier-Augen-Freigaben und werden in Architekturentscheidungsprotokollen dokumentiert. Die Wirksamkeitsprüfung erfolgt mehrstufig: statische Validierung der Policies vor Rollout, synthetische Erreichbarkeitstests je Zone (nur erlaubte Pfade sind erreichbar), aktive Messungen von Latenz, Paketverlust und Zeitdrift auf Föderationsstrecken sowie Sicherheitsdrills (Snapshot-Restore, Schlüsselrotation, Quarantäne-Importe, HIL-Negativtests). Ergebnisse werden als Evidenz in AAR-Paketen referenziert oder, falls höher eingestuft, im Vault abgelegt und lediglich nachweislich verlinkt.

Messbare Prüfkriterien sichern die Objektivität der Bewertung. Für Segmentierung gilt, dass ausschließlich die zuvor definierten Flussregeln erfüllt sind, keinerlei Transitverkehr zwischen Management- und Übungs-Zone außerhalb der Gateways detektiert wird und die Observability keinen Rückkanal in Workloads aufweist. Für Air-Gap ist der Disconnect-Test bestanden und die Protokolle sind frei von externen Abhängigkeiten. Für Föderation ist nachzuweisen, dass sämtliche Verbindungen über dedizierte VRF/VPN-Strecken mit beiderseitiger mTLS-Authentisierung und kurzlebigen Schlüsselmaterialien aufgebaut wurden, dass die vertraglich vereinbarten Austauschprofile und Zeitdrift-Toleranzen eingehalten sind und dass bei Grenzwertverletzungen definierte Degradationsmodi oder automatische Entkopplung gegriffen haben. In B gelten zusätzlich SLOs zur Policy-Durchsetzung im Mesh und zu Namespace-Isolation, während in A die Konsistenz der VRF/VLAN-Zuweisungen und Gateway-Regeln im Fokus steht.

4.9.2 Identität & Zugriff

Die Plattform verfolgt für Identität und Zugriff ein konsistentes Zero-Trust-Paradigma, das drei Ebenen unterscheidet: Menschen-Identitäten (Nutzer:innen), Dienst-/Workload-Identitäten sowie Gerätestatus (z. B. Jump-Hosts). Authentisierung und Autorisierung sind grundsätzlich mehrstufig, zeitlich begrenzt und policy-gesteuert. Damit lassen sich Air-Gap-Betrieb, Föderationskopplungen und starke Nachweisfähigkeit (Non-Repudiation) zugleich gewährleisten.

Für Useridentitäten wird ein lokal betriebener Identity Provider (IdP) gespeichert, der standardkonforme Protokolle (OIDC/SAML) unterstützt und vollständig offline funktionsfähig ist. Anmeldeverfahren nutzen vorzugsweise starke Faktoren (z. B. Smartcard/PIV oder FIDO2), die Ausgabe kryptographischer Tokens (z. B. signierte JWT) erfolgt mit kurzen Gültigkeitsdauern und eingeschränkten Scopes. Tokenvalidierung stützt sich auf lokal gespiegelt bereitgestellte JWKS-Schlüssel, und Zertifikatswiderrufe werden über offline gepflegte CRLs (bzw. OCSP-Ersatzmechanismen) durchgesetzt. Das Rollenmodell (RBAC) ist minimal und dienstspezifisch; es umfasst mindestens Trainer:in/Übungsleitung, Teilnehmer:in, Beobachter:in und Plattform-Ops. Rollen werden durch Mandanten- und Run-Scopes weiter eingeschränkt (z. B. Sicht auf die eigene Klasse/den eigenen Run). Für sicherheitskritische Aktionen—dazu zählen Start/Stop/Eskalation von Runs, Promotion von Artefakten sowie Schlüsselrotation—gilt Vier-Augen-Freigabe (Dual Control) mit verpflichtender Begründung und lückenloser Protokollierung. Temporäre Privilegien werden nach dem Just-in-Time-Prinzip vergeben und verfallen automatisch (Time-Boxing). Notfallzugänge („Break-Glass“) sind möglich, jedoch streng technisch abgesichert: Sie benötigen zwei unabhängige Autorisierende, werden gesondert markiert und unterliegen einer nachträglichen Audit-Prüfung.

Dienst- und Workload-Identitäten unterscheiden sich zwischen den Referenzarchitekturen in der technischen Ausprägung, verfolgen aber dieselben Sicherheitsziele. In Architektur B (Kubernetes/Service-Mesh) sind SPIFFE/SPIRE der Standard: Ein lokaler SPIRE-Server stellt

Workload-Identitäten (SVID-Zertifikate) aus, die durch Workload-Attestation (z. B. Node-, Pod- oder Label-Bedingungen) gebunden sind. Das Service-Mesh (mTLS by default) verwendet diese SVIDs für beidseitige Authentisierung und fein-granulare Autorisierung (Intent- und AuthZ-Policies auf Service-/Namespace-Ebene). SVIDs haben kurze TTLs und werden automatisch rotiert; Ableitungen in Policy-Claims (z. B. Mandant, Run-Scope, Rolle) erlauben autorisierte Flüsse ausschließlich entlang explizit freigegebener Pfade. Admission-Controller (z. B. OPA/Gatekeeper, Kyverno) erzwingen „controls-as-code“: nur signierte Images, verbotene Capabilities blockiert, korrekte Sidecars vorhanden, Netz-Policies wirksam. In Architektur A (VM-zentriert) übernehmen Host-/Service-Zertifikate (X.509) die mTLS-basierte gegenseitige Authentisierung auf Transportebene; VRF/VLAN-Segmentierung, Gateway-ACLs und Host-Firewalls stellen die Äquivalente zu Namespace-/Mesh-Policies dar. Autorisierungsentscheidungen basieren auf Zertifikat-Attributen (z. B. SAN/OU), signierten Konfigurationsprofilen und zentralen Policy-Regeln an den Gateways; auch hier sind Zertifikate kurzlebig und rotationsfähig, Widerrufe werden offline verifiziert.

Die Durchsetzung erfolgt entlang eines klaren Ablaufs (Abbildung 27). (1) Enrollment: Nutzer:innen und Services werden in der lokalen Vertrauensdomäne registriert (IdP-Directory, SPIRE-Registrierung, X.509-CA). (2) Ausstellung: Der IdP gibt signierte, kurzlebige Tokens mit minimalen Scopes aus; SPIRE bzw. die CA stellt kurzzeitige Zertifikate für Workloads/Dienste aus. (3) Zugriffsentscheidung: Jede Plattform-API und jedes Gateway verlangt mTLS und prüft RBAC/Policies; in B zusätzlich Mesh-Policies (Service-zu-Service). (4) Laufzeit-Governance: Tokens/Zertifikate werden automatisch rotiert; CRLs/JWKS werden offline synchronisiert; Abweichungen (z. B. abgelaufene SVIDs, ungültige Signaturen) führen fail-closed zum Verwerfen der Anfrage. (5) Protokollierung & Audit: Alle AuthN/AuthZ-Ereignisse, Policy-Entscheidungen und Ausnahmen werden append-only erfasst, mit UTC-Zeitstempel aus lokaler Quelle versehen und run-gebunden korreliert; für kritische Vorgänge wird zusätzlich die Freigabekette (wer/warum/wann) aufgezeichnet.

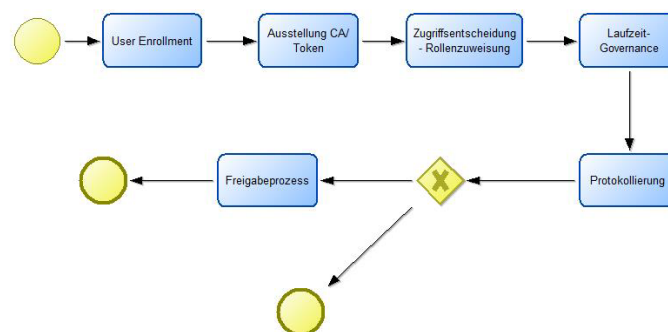


ABBILDUNG 27 ZUGRIFFSPROZESS

Die Ausgestaltung ist auditierbar und messbar. Mindest-SLOs umfassen: 100 % mTLS-erzwungene API-Zugriffe; Ablehnung unsignierter oder abgelaufener Tokens/Zertifikate; automatische Rotation innerhalb definierter Fristen; vollständige Journalisierung aller kritischen Aktionen; regelmäßige Access-Reviews (Rollenzuordnung vs. Aufgaben), Re-Zertifizierungen für privilegierte Konten sowie Disconnect-Nachweise (24 h ohne externe Abhängigkeiten, inkl. IdP-/CRL-/JWKS-Pfad). Testfälle schließen Negativszenarien ein: abgelaufene/gesperrte Zertifikate, widerrufene Schlüssel, ungültige SVIDs, fehlende Sidecars, nicht konforme Images oder unzulässige Scope-Elevations. In Föderationsszenarien werden Identitäten domänenübergreifend

abgebildet (Mapping-Profile), Schlüssel sind kurzlebig und kontextgebunden, und der Zugang ist auf die dedizierten Föderations-VRFs/VPNs beschränkt; Evidenzen liegen außerhalb des AAR in höherer Schutzstufe und werden dort versioniert und signiert.

4.9.3 Härtung der Plattform

Ziel der Baseline-Härtung ist die systematische Reduktion der Angriffsfläche bei gleichzeitiger Sicherstellung reproduzierbarer Zustände. Auf Host-Ebene umfasst dies ein minimales Betriebssystemprofil (deaktivierte optionale Pakete/Services), restriktive Benutzer- und Rechtekonfiguration, gehärtete Kernel-Parameter (z. B. `net.ipv4.conf.*.rp_filter=1`, `kernel.kptr_restrict=2`, `fs.protected_hardlinks=1`, `fs.protected_symlinks=1`, `kernel.unprivileged_bpf_disabled=1`) sowie das Sperren unnötiger Kernelmodule und Debug-Schnittstellen. Kryptographie wird über FIPS-taugliche Algorithmen/Module bereitgestellt; die Auswahl und Konfiguration erfolgen deterministisch über Policies-as-Code und werden regelmäßig verifiziert. Integritätsprüfungen (Package-Signaturen, File-Integrity-Checks) und sichere Protokollierung (append-only, UTC-Zeitbasis) sind Bestandteil der Grundhärtung.

Auf Workload-Ebene werden Container/VM-Gäste nach dem Prinzip „least privilege“ betrieben: read-only Root-Filesystem, kein „root“ im Container, seccomp-Profil und AppArmor/SELinux-Kontexte, Entfernung nicht benötigter Linux-Capabilities (z. B. `CAP_SYS_ADMIN`, `CAP_NET_RAW`), restriktive Volume-Mounts sowie—wo möglich—distroless- bzw. minimalistische Images. Geheimnisse werden nicht ins Image gebacken, sondern zur Laufzeit aus einem Tresor bezogen; Tools für Debugging oder Kompilierung sind nicht enthalten. Für beide Ebenen gelten wiederholbare, offline durchführbare Härtungsprüfungen (z. B. CIS-Benchmark-abgeleitete Checks), deren Ergebnisse als Evidenz versioniert werden.

Architektur-Spezifika. In A (VM-zentriert) stehen Host-Härtung (Hypervisor/Guest-OS), Host-Firewalls, abgeschaltete Verwaltungsdienste und kontrollierte Jump-Hosts im Fokus; Golden-Images (s. u.) bilden die technische Tragekonstruktion. In B (Kubernetes) werden die o. g. Maßnahmen zusätzlich durch Admission-Kontrollen (z. B. OPA/Gatekeeper, Kyverno) erzwungen: Nur signierte, policy-konforme Workloads mit gültigen seccomp/AppArmor-Profilen und ohne verbotene Capabilities werden zugelassen; Sidecar-Anforderungen des Service-Mesh sind verpflichtend.

Nachweis & Metrik. Akzeptanzkriterien umfassen u. a. 100 % erfolgreiche Härtungs-Checks vor Promotion, keine verbotenen Capabilities, vollständige Protokollierung sicherheitsrelevanter Ereignisse, sowie periodische Re-Validierung nach Patches. Abweichungen führen fail-closed zur Blockierung des Deployments.

4.9.3.1 Netz-Härtung (Segmentierung, Mikrosegmentierung, „Default-Deny“)

Die Netz-Härtung setzt „default deny“ an allen Zonengrenzen durch und erlaubt ausschließlich explizit genehmigte Flüsse. In A erfolgt die Makro-Segmentierung über VRF/VLAN und Gateway-ACLs; Anti-Spoofing-Regeln, strenge Egress-Kontrollen (Proxy/Allow-Lists) und Zonen-Guards (insb. für HIL/Föderation) sind verbindlich. Host-Firewalls (z. B. `nftables`) spiegeln diese Regeln auf den Endsystemen. In B ergänzen Kubernetes-NetworkPolicies die Makro-Segmentierung um Mikrosegmentierung auf Pod-Ebene; das Service-Mesh erzwingt mTLS-by-default mit Workload-Identitäten (SPIFFE/SVID) und stellt Intent/AuthZ-Policies für Service-zu-Service-Kommunikation bereit (u. a. L4/L7-Filter, Traffic-Shaping, Fault-Injection für DR-Tests). DNS- und NTP-Quellen sind lokal; Egress ist standardmäßig gesperrt. Föderationsverkehr verläuft ausschließlich über dedizierte VRF/VPN-Strecken mit kurzlebigen Schlüsseln; Realgeräte-Verbindungen passieren HIL-Guards mit Positiv/Negativ-Tests und Rate-Limits.

Nachweis & Metrik. Eine Reachability-Matrix belegt, dass nur freigegebene Pfade erreichbar sind; „any-to-any“ ist ausgeschlossen. Disconnect-Tests (≥ 24 h) müssen ohne externe Abhängigkeiten bestehen. In Föderationsszenarien sind mTLS-Handshake-Evidenzen, QoS-Kompatibilität und Zeitdrift im Toleranzband nachzuweisen; Grenzwertverletzungen lösen definierte Degradationsmodi oder automatische Entkopplung aus.

4.9.3.2 Delivery-Härtung (Lieferkette, Golden-Images/OCI-Artefakte, WORM)

Delivery-Härtung adressiert die Supply-Chain-Integrität von der Erstellung bis zur Auslieferung. In A ist eine Golden-Image-Politik maßgeblich: deterministische Builds (z. B. via Packer) erzeugen OVAs mit fixierten Paketquellen/Versionen; jedes Image trägt SBOM (SPDX/CycloneDX), sha256-Digest und eine digitale Signatur. Freigaben erfolgen erst nach drei identischen Rebuilds (Hash-Gleichheit), bestandenen Offline-Malware-Scans, Härtings- und Funktionstests. Images werden in einem immutablen Mirror mit WORM-Eigenschaft abgelegt; Promotionen erfolgen stufenweise (Quarantäne → Staging → Produktion) und sind vollständig rückrollbar.

In B gilt Entsprechendes für OCI-Artefakte (Container-Images, Charts). Artefakte sind reproduzierbar gebaut, signiert (z. B. Cosign) und mit In-Toto/Provenance attestiert; die SBOM-Pflicht ist Gate-Kriterium. Eine Quarantäne-Stufe prüft Signaturen, Digests und Schwachstellen (offline-fähige Scanner) und erzwingt Richtlinien (verbotene Basen, kritische CVEs) vor Aufnahme ins lokale Registry-Mirror. Admission-Policies im Cluster verwehren nicht signierte oder nicht-konforme Artefakte; nur Digest-gepinntes Pulling ist zulässig. Charts/Manifeste sind versions- und signaturgebunden; GitOps-Controller synchronisieren ausschließlich geprüfte Commits.

Nachweis & Metrik. Pflichtnachweise sind (i) lückenlose Signatur-/SBOM-Ketten, (ii) dokumentierte, erfolgreiche Quarantäne-Prüfungen, (iii) reproduzierbare Builds, (iv) Audit-Protokolle der Promotionen und (v) WORM-Belege. Ein Verstoß in beliebiger Stufe führt fail-closed zur unmittelbaren Sperrung des Artefakts.

4.9.4 Schlüsselverwaltung, Rotation, Tresor

Die Plattform verfolgt für klassifiziertes und kryptographische Schlüssel einen strikt evidenzbasierten Ansatz, der Vertraulichkeit, Integrität und Nichtabstreitbarkeit unter Offline-Bedingungen sicherstellt. Leitprinzipien sind „least knowledge“ (minimale Einsicht in Geheimnisse auch für privilegierte Rollen), „short-lived by default“ (kurzlebige, kontextgebundene Tokens/Zertifikate) und „controls-as-code“ (maschinlesbare Richtlinien für Ausstellung, Nutzung und Widerruf). Sämtliche Prozesse sind reproduzierbar, revisionssicher und deterministisch testbar.

Tresorumgebung. Zentrale Tresorumgebung sind die lokale PKI/CA, die Zeitquelle und die föderationsspezifischen Schlüssel. Die PKI/CA wird offline-fähig betrieben; Root-CAs verbleiben vollständig isoliert, Sub-CAs werden für betriebliche Zwecke zeitweise aktiviert und anschließend sicher versiegelt. Die Zeitquelle (NTP Stratum-1 mit GPS, optional PTP) dient als Referenz für Signatur- und Widerrufszeitstempel sowie für die zeitliche Korrelation von Audit-Ereignissen. Föderations-Keys (z. B. für mTLS-Strecken oder HLA/DDS-Bridges) sind kurzlebig und kontextgebunden (Run/Session). Alle hochschutzbedürftigen Materialien werden in einer Tresorumgebung mit Hardware-Unterstützung (HSM/TPM) gehalten; Schlüsseloperationen (Key-Gen, Sign, Unseal) sind nur über streng kontrollierte Schnittstellen erlaubt, die ihrerseits mTLS, RBAC und Vier-Augen-Freigaben durchsetzen. Für die Software-Schicht empfiehlt sich ein dedizierter Vault-Dienst im „sealed“ Modus; Auto-Unseal erfolgt über HSM-gestützte Key-Shares, sodass „Secret-Zero“ effektiv vermieden wird.

Lebenszyklus und Kryptoprofile. Der Lebenszyklus umfasst Erzeugung, Ausstellung, Verteilung, Nutzung, Rotation, Widerruf, Archivierung und Vernichtung. Schlüssel werden auf der

vertrauenswürdigen Seite mit genügend Entropie erzeugt; zulässige Algorithmen sind—abhängig von Vorgaben—z. B. Ed25519 oder ECDSA P-256 für Signaturen sowie RSA-3072 für Kompatibilitätspflichten. Für Transport wird TLS 1.3 mit Perfect Forward Secrecy erzwungen; Cipher-Suites und EKUs werden profilbasiert eingeschränkt. Zertifikatsprofile definieren erlaubte SANs (DNS/URI), KeyUsage/ExtendedKeyUsage, maximale Gültigkeitsdauern sowie zulässige Pfadlängen. Rotation erfolgt zeitgesteuert (kurze TTLs) oder ereignisgesteuert (Compromise-Signale); Widerrufe werden über offline gepflegte CRLs bzw. OCSP-Ersatzmechanismen propagiert. Alle Übergänge erzeugen signierte, WORM-gespeicherte Ereignisse (Wer/Wann/Womit), die über die lokale Zeitbasis deterministisch verifizierbar sind.

Secret-Handling und Verteilung im Air-Gap. Geheimnisse sind strikt vom Code getrennt und werden nur zur Laufzeit eingebracht („late binding“). Persistenz erfolgt ausschließlich verschlüsselt; Zugriff ist fein-granular (RBAC, Mandant/Run-Scope) und protokolliert. In Air-Gap-Betrieb werden JWKS, CRLs und Policy-Bundles lokal gespiegelt und mit geprüften, physisch transferierten Snapshots aktualisiert (Quarantäne → Signatur/SBOM-Prüfung → Promotion). Verteilung folgt dem Pull-Prinzip aus der Vertrauensdomäne: Workloads authentisieren sich per mTLS gegenüber dem Tresor und erhalten kurzlebige Credentials, die automatisch erneuert werden; statische „Long-Term Secrets“ sind untersagt. Schlüssel im Anwendungskontext werden—wo möglich—per Envelope-Encryption gehandhabt, sodass kompromittierte Speichermedien ohne Zugriff auf den Master Key wertlos bleiben. Break-Glass-Zugänge sind technisch gebunden an Mehr-Augen-Freigaben und erzeugen gesonderte, unüberschreibbare Audits.

Architekturspezifika A vs. B. In Architektur A (VM-zentriert) liegen die Schwerpunkte auf Host- und Dienstzertifikaten (X.509) für mTLS an Gateways, Hypervisor- und Gast-Härtung sowie Golden-Image-Disziplin. Secrets werden über den Vault/Tresor auf Hosts oder in dedizierten Management-VMs injiziert; Host-Firewalls und VRF/VLAN-Isolierung fungieren als technische Rückfallebene. In Architektur B (Kubernetes/Service-Mesh) sind SPIFFE/SPIRE der Standard für Workload-Identitäten: SVIDs ersetzen statische Secrets, werden durch Workload-Attestation gebunden und besitzen kurze TTLs. Admission-Controller (z. B. OPA/Gatekeeper, Kyverno) erzwingen Signatur- und Policy-Pflichten, CSI-Secret-Driver und External-Secrets-Operator sorgen für rotierende, versionsgebundene Materialisierung. Das Service-Mesh stellt Ende-zu-Ende-mTLS und Autorisierungsentscheidungen bereit; die Tresorumgebung bleibt die Quelle der Wahrheit.

Betrieb, Governance und Forensik. Schlüssel- und Secret-Prozesse sind als Runbooks und ADRs dokumentiert: Key-Ceremonies (inkl. Teilnehmende, Quoren, Protokolle), Rotations- und Rollover-Verfahren (mit Grace-Periods), Widerrufsprozesse, Notfallpfade und Entsorgungsrichtlinien (z. B. sichere Vernichtung von Medien). Backups hochkritischer Materialien (Root/Intermediate Keys, Vault-Master) erfolgen verschlüsselt und geographisch getrennt; Threshold-Verfahren (z. B. Shamir) minimieren Insider-Risiken. DR-Ziele sind definiert (z. B. RTO < 2 h für Sub-CA/Wiederanlauf, RPO ≤ 15 min für Metadaten), und regelmäßige Restore-Drills belegen die Rekonstitutionsfähigkeit. Audits stützen sich auf WORM-gespeicherte, signierte Protokolle (Ausstellung, Nutzung, Rotation, Widerruf), die über die lokale Zeitquelle verifiziert werden; Abweichungen führen fail-closed zur Sperrung betroffener Artefakte und Verbindungen.

Messbare Akzeptanzkriterien. Minimalanforderungen umfassen (i) 100 % mTLS-erzwingende Schlüsselpfade; (ii) ausschließlich kurzlebige Zertifikate/Tokens im Produktionsbetrieb; (iii) vollständige Journalisierung aller Schlüsseloperationen; (iv) Rotations-SLOs (z. B. < 5 Min. bis zur Propagation eines Widerrufs in allen relevanten Zonen); (v) keine Secrets im Klartext-Repo, keine statischen Zugangsdaten in Images; (vi) erfolgreiche, protokollierte DR-Drills gemäß Zielwerten. Für föderierte Übungen gilt zusätzlich: kurzlebige, kontextgebundene Föderations-Keys, dokumentierte Handshake-Evidenzen und nachweislich minimalisierte Exportsichten.

4.9.5 Protokollierung, Observability & Audit

Die Protokollierungs- und Beobachtbarkeitsarchitektur der Plattform verfolgt drei Ziele: 1) Die lückenlose, manipulationsresistente Erfassung sicherheits- und betriebsrelevanter Ereignisse; 2) Die Run-gebundene, performante Analyse von Metriken, Logs, Events und Traces (MELT) zur didaktischen Steuerung und forensischen Auswertung; 3) Die Ableitung auditfester Evidenzpakete (AAR), ohne hochschutzbedürftige Details unnötig breit zu streuen. Sämtliche Mechanismen sind offline funktionsfähig, deterministisch testbar und durch Policies-as-Code technisch erzwungen.

Protokollierung erfolgt zentral, zeitkonsistent und append-only. Alle Ereignisse werden mit UTC-Zeitstempeln aus einer lokalen Stratum-Quelle versehen; dadurch bleiben Reihenfolge und Kausalität auch in föderierten oder air-gapped Szenarien nachvollziehbar. Die Logaufnahme trennt klar zwischen einer Sicherheits-Taxonomie (u. a. Authentisierung/Autorisierung, Policy-Entscheidungen, Konfigurationsänderungen, Orchestrierungsbefehle, Föderations-Handshakes, HIL-Guard-Ereignisse, Exporte/Imports) und einer Betriebs-Taxonomie (z. B. Bereitstellungsphasen, Ressourcen-Quoten, Health-Checks, Ingest-Latenzen). Ereignisse werden strukturiert (JSON-Zeilenformat) mit Schema-IDs, run_id, Mandant/Run-Scope und Quelle (component) erfasst; optionale Hash-Ketten bzw. Merkle-Bäume können zur zusätzlichen Unveränderbarkeitsprüfung eingesetzt werden. Die Ablage ist in Hot/Warm/Cold/WORM-Tiers organisiert: Hot für niedrige Latenzen (Dashboards, Ad-hoc-Analysen), Warm für aggregierte Sichten, Cold/WORM für revisionssichere Langzeitbeweise. Schreibpfade sind „append-only“ (z. B. durch unveränderliche Objekt-Buckets oder linuxseitige Append-Schutzmechanismen); Retention, Legal-Hold und Löschprozesse sind dokumentiert, getestet und schließen Backups ein.

Observability wird run-gebunden betrieben: Jeder Datensatz trägt die run_id als primären Korrelationsschlüssel, wodurch Telemetrie (OTLP für Metriken/Logs/Traces, Syslog für Systemereignisse, NetFlow/IPFIX für Netzflüsse, DDS/HLA für Simulationsdaten) deterministisch einem Szenario-Durchlauf zugeordnet bleibt. Attributnamen und Wertebereiche sind pro Quelle kanonisiert, schema-versioniert und pipeline-integriert validiert (fail-closed). Kardinalitätsbudgets, Abfrage-SLOs und Ingest-Latenzen werden als Betriebsziele überwacht; für Standard-Sichten ist ein P95 unter zwei Sekunden vorgesehen, die Ingest-Pipeline hält definierte Obergrenzen für Verzögerung und Verlustquote ein. Die Observability-Zone ist „write-controlled“ ausgelegt: Sie nimmt Daten aus Übungs- und Föderationszonen entgegen, exponiert jedoch keinen Rückkanal in Workloads. In Referenzarchitektur A erfolgen Ingest und Agentisierung host- bzw. VM-basiert; in B ergänzen Mesh-Sidecars und Workload-Identitäten (SVID) eine feingranulare Ende-zu-Ende-Zuordnung von Flüssen und Policies.

Das AAR-Konzept bündelt die für Nachweis und Lehre relevanten Informationen in signierten Manifesten mit Hashes, SBOM-Fingerprints und Referenzen auf Run-Ereignisse und Artefakte. Hochschutzbedürftige Inhalte—insbesondere Schlüsselmaterial, Föderationsverträge und detaillierte Mapping-Profile—werden nicht in das AAR eingebettet, sondern ausschließlich referenziert; die zugrunde liegenden Belege liegen in höherer Schutzstufe (z. B. Federation-Vault) WORM-fähig vor. AAR- und Audit-Ablagen sind unveränderlich konfiguriert; jede Änderung am Status (Promotion, Sperrung, Depublizierung) erzeugt ihrerseits einen signierten Audit-Eintrag. Für personenbezogene Daten gelten Datenminimierung, Pseudonymisierung und dokumentierte Maskierungsregeln; Klassifizierungslabes werden entlang der Referenzen vererbt, sodass ein AAR mindestens die höchste Schutzstufe seiner referenzierten Komponenten annimmt.

Auditfähigkeit entsteht aus z.B. mit Controls-as-Code. Admission- und Governance-Policies (in A z.B. Host-/Gateway-Regeln, in B zusätzlich OPA/Gatekeeper/Kyverno und Mesh-Intent) sind versioniert, signiert und vor Rollout statisch validiert; nur konforme Workloads/Artefakte werden zugelassen. Releasenachweise (signierte ADRs, Freigabeprotokolle, Build-Provenienz) schließen die Lücke zwischen Änderung und Betrieb; jede kritische Aktion (Start/Stop/Eskalation, Artefakt-



Promotion, Schlüsselrotation) unterliegt Vier-Augen-Freigaben, ist vollständig journalisiert und rungebunden korreliert. Regelmäßige Disconnect- und Restore-Drills belegen die Rekonstitutionsfähigkeit (RTO/RPO-Ziele) und werden als AAR archiviert; Messgrößen umfassen u. a. Validierungs- und Ingest-Latenzen, Query-SLO-Einhaltung, Policy-Trefferquoten, Zeitdrift in Föderationen und Fehlerraten nach Ursachenklassen. Abweichungen führen fail-closed zur Quarantäne von Daten oder zur automatischen Entkopplung von Strecken (z. B. in der Föderationszone), bis eine signierte Freigabe erfolgt.

4.9.6 Policies-as-Code & Compliance-Nachweis

Die Plattform verankert Sicherheits-, Daten- und Föderationsregeln als Policies-as-Code. Dadurch werden normative Vorgaben maschinenlesbar, versionier- und testbar, und ihre Durchsetzung ist reproduzierbar nachweisbar. In Referenzarchitektur B (Kubernetes) erfolgt die Policy-Durchsetzung mehrstufig: Admission-Kontrollen (z. B. OPA/Gatekeeper oder Kyverno) prüfen eingehende Ressourcen gegen signierte Policy-Bundles (Rego/CRD-Regeln), Service-Mesh-Policies erzwingen mTLS-by-default und erlauben nur explizit genehmigte Service-zu-Service-Beziehungen, und NetworkPolicies begrenzen Datenpfade auf Namespace-/Pod-Ebene. In Referenzarchitektur A (VM-zentriert) übernehmen signierte Host-/Firewall-Policies, Gateway-ACLs und VRF/VLAN-Zuweisungen die äquivalente Rolle; auch hier werden Regelwerke versionsgebunden gepflegt und vor dem Rollout statisch verifiziert.

Die Lieferkette für Policies folgt denselben Prinzipien wie für Code und Artefakte: semantische Versionierung, signierte Commits/Tags, Vier-Augen-Freigaben und Promotion über Quarantäne – > Staging –> Produktion. Policy-Bundles tragen einen kryptographischen Digest und eine (ggf. separate) Signatur; der ausgerollte Stand wird in Metadaten von Deployments, Jobs oder Gateways referenziert. Pipelines und Ingest-Gates arbeiten fail-closed: Liegt bei Schema-, Policy- oder Signaturprüfungen kein positives Ergebnis vor, wird die Operation blockiert, in Quarantäne verschoben und mit strukturierten Fehlern (Regel, Fundstelle, erwarteter vs. beobachteter Zustand) protokolliert. Für föderierte Strecken werden Austauschprofile (Exportsichten, QoS, Namensräume) ebenfalls als Code geführt; die zugehörigen Mapping-Validatoren prüfen Schema- und QoS-Kompatibilität vor Aktivierung der Verbindung.

Der Compliance-Nachweis wird über zwei Artefaktgruppen erbracht. Erstens dokumentieren ADRs/RFCs (als signierte, versionierte Dokumente) die Ableitung der Policies aus internen Vorgaben oder behördlichen/branchenspezifischen Anforderungen (z. B. Zuordnung von Controls zu Paragraphen/Controls-Katalogen). Zweitens liefern Dashboards laufende KPI/SLO-Nachweise, u. a. Validierungslatenz, Policy-Trefferquoten, Ablehnungsgründe, Ingest- und Query-SLOs sowie Föderations-Drift-Metriken. Die Chain-of-Custody bleibt geschlossen, da jede Policy-Änderung, jeder Gate-Entscheid und jede Promotion signiert, zeitgestempelt (lokale Stratum-Quelle) und WORM-fähig archiviert wird. Ausnahmeverfahren („Policy-Break-Glass“) sind möglich, aber dual kontrolliert, streng zeitlich begrenzt und obligatorisch nachzuberichten (Post-Event-Review mit Ursachenanalyse und Korrekturmaßnahme).

4.9.7 Unterschiede/„Deltas“ zwischen Referenzarchitektur A und B

Segmentierung. Architektur A setzt auf Hypervisor-Isolierung und VRF/VLAN als Primärmechanismen; Flüsse werden an Gateway-Rändern mit ACLs und mTLS kontrolliert. Architektur B ergänzt die Makro-Segmentierung um Namespace-Isolation, NetworkPolicies und Service-Mesh-Policies; dadurch entsteht Mikrosegmentierung bis hin zur einzelnen Workload-Beziehung mit erzwingbarem mTLS-by-default. Operativ bedeutet dies: A bietet hohe Stabilität und einfache Sichtbarkeit der Pfade auf Netzwerkebene, B ermöglicht feinere, dynamische Steuerung auf Dienstebene (dafür steigt der Policy- und Betriebsaufwand).



Identitäten. In A dominieren X.509-Dienstzertifikate für beidseitige Authentisierung (Gateways/Hosts); Autorisierung stützt sich auf Zertifikat-Attribute und zentrale Policy-Sets. In B stellen SPIFFE/SPIRE Workload-Identitäten (SVID) bereit; das Mesh nutzt sie für AuthN/Z-Entscheide, Sidecar-gestützt und mit kurzen TTLs. Ergebnis: B erreicht Zero-Trust-Granularität bis zum Pod/Service, A bleibt host-/dienstzentriert und einfacher in stark gekapselten Umgebungen.

Härtung & Delivery. A nutzt Golden-Images/OVAs mit deterministischen Rebuilds, Offline-Malware-Scans, SBOMs und Signaturen; Promotion erfolgt in ein immutables OVA-Mirror (WORM). B setzt auf OCI-Artefakte (Container/Charts), GitOps-Synchronisation und Admission-Gates; nur signierte, policy-konforme Workloads werden zugelassen. Beide Varianten erzwingen reproduzierbare Builds und signierte Lieferketten; B skaliert Änderungen schneller, A begünstigt streng deterministische Zustände.

Föderation. A nutzt HLA/DIS als Kernstandards und kapselt Verkehre in dedizierten VRF/VPN-Strecken. B verwendet DDS-Domänen als Datenbus und koppelt HLA über eine Bridge; Mesh-gestützte ACLs und SVID-Identitäten erlauben feinere Exportkontrolle. In beiden Fällen sind Schlüssel kurzlebig und Export-Sichten minimal; die Nachweise (Handshake, Mapping, Drift) liegen außerhalb des AAR in höherer Schutzstufe.



4.10 Bereitstellung, Betrieb & Support

Dieses Kapitel operationalisiert die Referenzarchitekturen A und B für den produktiven Trainingsbetrieb unter Air-Gap-Bedingungen. Im Mittelpunkt steht ein normativer Betriebskanon aus dokumentierten Runbooks (Provisionierung, Day-2-Operations, Backup/Restore, Disaster Recovery), wohldefinierten Offline-Prozessen (Artefakt-Transport, Patch-Fenster, Schlüsselrotation) sowie formalisierten SLA/SLOs und Regeln der Kapazitätsplanung. Die Maßnahmen sind als controls-as-code ausgestaltet, versioniert und signiert und bilden damit eine überprüfbare Brücke zwischen Architekturentwurf (Kapitel 4.5 und 4.6), Schnittstellen-/Datenkonsolidierung (Kapitel 8) und Sicherheits-/Compliance-Anforderungen (Kapitel 4.8.3).

Ziel ist ein deterministischer, auditierbarer und air-gap-fähiger Lebenszyklus, der die Muss-Kriterien der Plattform, Offline-Betrieb ohne externe Abhängigkeiten, föderationsfähige Kopplung, reproduzierbare Bereitstellung, AAR-Evidenz, messbar erfüllt. Hierzu beschreiben die Runbooks nicht nur Abläufe, sondern auch Eingangs- und Ausgangsbedingungen, Gating-Prüfungen, Rollback-Mechanismen und Akzeptanzkriterien. Alle Entscheidungen werden rollenbasiert (Trainer:in/Übungsleitung, Plattform-Ops) und mit Vier-Augen-Freigaben für kritische Schritte (Netz-Änderungen, Artefakt-Promotion, Schlüsselrotation) vollzogen; Zustands- und Freigabespuren fließen in AAR-Pakete bzw, bei höherem Schutzbedarf, in gesonderte, WORM-fähige Audit-Ablagen ein.

Die Offline-Prozesse normieren die Versorgungskette im Air-Gap: Artefakte passieren eine Quarantäne-Stufe mit Signatur-, Hash- und SBOM-Prüfung sowie Offline-Malware-Checks; Promotionen verlaufen stufig Quarantäne → Staging → Produktion und sind jederzeit rückrollbar. Patch-Fenster werden risikobasiert gebündelt und durch End-to-End-Tests abgesichert. Schlüsselrotation folgt kurzlebigen Gültigkeiten und atomaren Umschaltverfahren. Sämtliche Key-Events werden in der Tresorumgebung journalisiert. Damit wird gewährleistet, dass sowohl Architektur A (Golden-Images/OVAs, VRF/VLAN-Segmente) als auch Architektur B (OCI-Artefakte, GitOps, Service-Mesh) ihre Sicherheits- und Reproduktionsziele betrieblich erzwingen.

Die SLA/SLO-Systematik verankert Qualitätsziele als technische Schranken in Pipeline und Betrieb und macht sie unabhängig prüfbar: Bereitstellungszeiten, Abfrage-Latenzen, Ingest-Verlustquoten, Verfügbarkeiten zentraler Dienste, Drift-Toleranzen auf Föderationsstrecken sowie Compliance-Trefferquoten werden kontinuierlich erhoben, gegen Sollwerte verglichen und im Fall von Abweichungen automatisiert geahndet. Die Kapazitätsplanung definiert deterministische Obergrenzen für parallele Übungsrunden aus konservativen Ressourcenprofilen je Szenario unter Einrechnung von Headroom und Plattform-Overheads; regelmäßige Kalibrierungen an realer Last sichern die Prognosegüte und schützen vor Noisy-Neighbor-Effekten.

Schließlich stellt das Kapitel die Governance-Einbettung sicher: Runbooks, Offline-Verfahren, SLO-Definitionen, Kapazitätsannahmen, Disconnect-/Restore-Drills und DR-Proben werden als ADRs versioniert, signiert und in AARs referenziert. Durch diese formale Klammer werden Aufbau, Änderung und Wiederherstellung der Trainingsplattform nicht nur reproduzierbar und nachweisbar, sondern auch vergleichbar über beide Referenzarchitekturen hinweg—und damit unmittelbar anschlussfähig an den Variantenvergleich (Kapitel 4.7) sowie die Sicherheits- und Compliance-Nachweise (Kapitel 4.8.3).

4.10.1 Runbooks

4.10.1.1 Provisionierung IaC

Die Provisionierung beschreibt den deterministischen Übergang von signierten Quellartefakten zu einer trainingsbereiten Zielumgebung. Sie ist als Infrastructure-as-Code-(IaC-)Prozess



ausgestaltet und bildet die Verbindung zwischen Architektur (Kapitel 4.5 und 4.6), Schnittstellen-/Datenmodellen (Kapitel 8) und Sicherheits-/Compliance-Kontrollen (Kapitel 4.8.3).

Eingangsgrößen und Vorbedingungen. Grundlage sind signierte und versionierte Artefakte: IaC-Definitionen (z. B. Terraform-Stacks, Ansible-Rollen,...), Images mit SBOM, Szenariobeschreibungen sowie Policies-as-Code. Vor dem Start liegen eine Ressourcenabschätzung, die Zonen-/Segmentierungsregeln (Kapitel 4.8.3), ein Rollenmodell mit RBAC-Scopes (Kapitel 4.8.3) und die Zeitbasis vor. Die Durchführung erfolgt durch Plattform-Ops; sicherheitskritische Schritte (Netzänderungen, Artefakt-Promotion) unterliegen dem Vier-Augen-Prinzip.

Phasenmodell und Gating (fail-closed).

1. Pre- Provisioning -Checks. Vor dem eigentlichen Rollout verifiziert der Prozess Signaturen und Hashes sämtlicher Artefakte (Images, Charts, Manifeste) und validiert Schemata/Policies der Szenariobeschreibungen. Parallel erfolgt eine Ressourcen-Vorprüfung gegen definierte Quotas (CPU/RAM/Storage/Netz). Jede Abweichung führt fail-closed zur Blockierung mit strukturiertem Fehlerprotokoll. Ergebnis ist ein signiertes Freigabeprotokoll oder ein begründeter Abbruch mit Quarantäne-Vermerk.
2. Plan. In der Planungsphase werden deterministische Baupläne erzeugt: Terraform-Plans (für A und B), gerenderte Helm/Kustomize-Manifeste (B) sowie Dry-Runs der Orchestrierung. Sämtliche Artefakte erhalten Digest/Hash und eine Schema-ID; Abhängigkeiten sind durch Version-Pinning fixiert. Ziel ist ein unstrittiger Soll-Zustand (‘intended state’), der gegen Policies-as-Code geprüft und für Audit-Zwecke archiviert wird.
3. Apply. Die Umsetzung erfolgt stufenweise: Zunächst Staging, anschließend Smoke-/Health-Checks. Erst bei Erfolg folgt die Promotion in Produktion. Jede Abweichung triggert einen automatischen Rollback auf den letzten bekannten, signierten Stand. Die Durchsetzung ist in A hypervisor-/gateway-zentriert (VRF/VLAN, Host-Firewalls, OVA-Images), in B cluster-/workload-zentriert (Admission-Gates, NetworkPolicies, Service-Mesh).
4. Post-Provisioning. Nach erfolgreichem Apply werden die bereitgestellten Ressourcen in der Orchestrierung registriert, Identitäten und RBAC-Scopes für Rollen und Workloads gebunden, Netz-Policies aktiviert und eine Baseline-Observability eingeschaltet. Die Umgebung gilt als „trainingsbereit“, wenn die SLO für Time-to-Train erreicht und alle obligatorischen Checks bestanden sind.
5. Abschluss & Evidenz. Den Abschluss bilden signierte Protokolle des gesamten Ablaufs, ein Version/Digest-Inventar sowie eine AAR-Referenz auf Build-/Deploy-Provenienz. Die Evidenz wird WORM-fähig archiviert; hochschutzbedürftige Belege (z. B. Föderations-Schlüssel/Handshakes) verbleiben im Vault und werden im AAR lediglich referenziert.

Fehlerbehandlung und Resilienzmechanismen. Der Prozess ist durchgängig transaktional konzipiert. In jeder Phase existiert ein definierter Abbruchpunkt mit sauberem Rückweg in den letzten reproduzierbaren Zustand. Pre-Provisioning-Fehler führen zur Quarantäne des betroffenen Artefakts. Plan-Konflikte werden nicht angewendet; es erfolgt eine Policy-gesteuerte Korrektur. Apply-Fehler lösen Rollback und Ursachenanalyse aus. Post-Provisioning-Fehler (z. B. fehlende Telemetrie) führen zu gezieltem Triage-Pfad und, falls notwendig, zum Graceful-Degradation-Modus.

Ausprägungsunterschiede A/B.



Architektur A: Schwerpunkt auf Golden-Images/OVAs, Snapshot/Clone-Funktionen, VRF/VLAN-Segmentierung und Gateway-Policies. IaC-Pfade umfassen Terraform, Ansible und Packer. Durch die strikte Image-Disziplin sind Zustandsübergänge besonders gut reproduzierbar; horizontale Elastizität ist begrenzt, dafür sind Air-Gap-Kontrollen sehr stabil.

Architektur B: Schwerpunkt auf OCI-Artefakten, GitOps-Synchronisation und Admission-Gates mit mTLS-by-default. Plans und Manifeste werden policy-gestützt validiert; Rollouts nutzen Canary/Blue-Green-Muster. Hohe Elastizität und feingranulare Policies erhöhen die Änderungssagilität, erfordern aber strenge Kardinalitäts- und Policy-Kontrollen.

Rollen, Kontrollen und Nachweisführung. Operative Verantwortung liegt bei Plattform-Ops; Übungsleitung/Trainer:in initiiert szenariobezogene Provisionierungen. Kritische Aktionen sind dual kontrolliert und werden mit UTC-Stempeln aus lokaler Quelle journalisiert. Jede Pipeline-Stufe besitzt Gates, arbeitet fail-closed und erzeugt Audit-Ereignisse für AAR und Vault. Damit wird die Chain-of-Custody über den gesamten Bereitstellungszyklus geschlossen.

4.10.1.2 Day-2-Operations

Day-2-Operations umfassen alle Tätigkeiten nach der Erstbereitstellung und sichern einen stabilen, konformen und planbaren Betrieb unter Air-Gap-Bedingungen. Zentrales Ziel ist die verlässliche Einhaltung des deklarierten Soll-Zustands, die vorausschauende Ressourcensteuerung, eine schnelle und forensisch nachvollziehbare Störungsbehandlung sowie ein kontrolliertes Änderungswesen. Alle Verfahren arbeiten fail-closed, erzeugen revisionssichere Evidenz und bleiben ohne externe Abhängigkeiten funktionsfähig.

Konfigurationsmanagement und Driftkontrolle gewährleisten, dass die reale Plattform jederzeit dem deklarativen Modell entspricht. In der VM-zentrierten Architektur A wird der Ist-Zustand kontinuierlich gegen Terraform-Zustände und Ansible-Profile geprüft; Abweichungen in Topologie, Härtung oder Gateway-Regeln führen zu einem blockierenden Befund mit anschließender, kontrollierter Remediation. Golden-Image-Disziplin verhindert dabei „Hot-Fixes“ am laufenden System: Änderungen werden grundsätzlich über den Build-/Promotionspfad rekonstituiert. In der Cloud-nativen Architektur B übernehmen GitOps-Controller die fortlaufende Reconciliation; Admission- und Mesh-Policies erzwingen Zero-Trust-Vorgaben auf Workload-Ebene und verwehren nicht konforme Ressourcen bereits beim Eintritt. In beiden Varianten wird die Wirksamkeit der Kontrollen anhand definierter Kennzahlen gemessen; jede Abweichung erzeugt einen signierten Audit-Eintrag und, sofern trainingsrelevant, einen Verweis im AAR.

Die Kapazitätssteuerung balanciert Parallelität, Isolation und Leistungsziele. Architektur A nutzt Ressourcengruppen und VRF/VLAN-basierte Platzierung mit konservativem Overcommit sowie festen Puffern für Klon- und Wiederherstellungsprozesse. Architektur B setzt auf Quotas und LimitRanges je Mandant bzw. Namespace; elastische Mechanismen bleiben an definierte Obergrenzen gebunden. Startentscheidungen für neue Runs werden grundsätzlich an Mindestressourcen geknüpft—reicht die Kapazität nicht, wird der Vorgang deterministisch abgelehnt. Prognosen kombinieren gemessene Profilwerte der Szenarien mit Headroom-Zuschlägen; Abweichungen zwischen Forecast und realer Last führen zu dokumentierten Kapazitätsmaßnahmen.

Incident-Response folgt einem strikt evidenzbasierten Ablauf. Diagnose und Triage stützen sich auf run-gebundene MELT-Sichten, wobei die run_id als primärer Korrelationsschlüssel dient. Bei Störungen werden Kommunikationspfade über Policies verengt, betroffene Runs geordnet pausiert und, wenn erforderlich, in Quarantäne-Segmente isoliert. Forensisch relevante Zustände werden in A durch Snapshots, in B über zustandsarme Artefakt-Exporte und Telemetrie-Sicherungen mit Hash/Signatur konserviert. Eskalation, Notfallpfade und Break-Glass-Zugänge sind dual

kontrolliert; Ergebnisse, Ursachen und Korrekturmaßnahmen werden als Post-Incident-AAR dokumentiert und in den Runbooks nachgezogen.

Änderungen erfolgen ausschließlich über einen stufigen Pfad und innerhalb planbarer Wartungsfenster. Artefakte passieren Quarantäne, Staging und erst nach bestandenen Prüfungen die Produktion; Rückrollpunkte sind vorab definiert. Architektur A nutzt hierfür Snapshots/Clones und rekonstruiert Systeme aus signierten Images, während Architektur B rollierende Deployments und Revisionsverwaltung nutzt, flankiert von Admission-Gates als letzter technischer Schranke. Für besonders kritische Übungsphasen gilt ein Änderungs-Freeze; Ausnahmen sind zeitlich eng begrenzt, begründungspflichtig und vollständig journalisiert.

Die Governance verankert Verantwortlichkeiten, Schwellenwerte und Nachweise. Plattform-Ops steuert Betrieb und Remediation; die Übungsleitung verantwortet szenariobezogene Entscheidungen wie Pausen oder Eskalationen. Für netzrelevante Änderungen, Artefakt-Promotionen und Schlüsselrotation gilt das Vier-Augen-Prinzip. Serviceziele werden kontinuierlich überwacht; Grenzwertverletzungen führen automatisch zu Quarantäne, Rollback oder Entkopplung betroffener Strecken. Sämtliche Ergebnisse fließen in AAR-Pakete und als ADRs in die Wissensbasis ein, sodass Day-2-Operations nicht nur stabilisieren, sondern den Betrieb über beide Referenzarchitekturen hinweg messbar und auditfest weiterentwickeln.

4.10.1.3 Backup/Restore

Backup/Restore stellt die Wiederherstellbarkeit betriebs- und nachweiskritischer Zustände sicher und erhält die forensische Beweiskette über den gesamten Lebenszyklus der Plattform. Der Fokus liegt nicht allein auf Datenkopien, sondern auf konsistenten, signaturgeprüften Zustandsabbildern samt Metadaten, aus denen sich sowohl Konfiguration und Laufzeit als auch AAR-Evidenz deterministisch rekonstruieren lassen—und zwar unter Air-Gap-Bedingungen.

Schutzumfang und Domänen. Gesichert werden (i) Konfigurations-/IaC-Repos einschließlich Policies-as-Code und Release-ADRs, (ii) Registry/Mirror-Kataloge mit Digests, Signaturen und SBOMs, (iii) Orchestrierungs- und AAR-Metadaten mitsamt Timeline-Indizes, (iv) PKI-/IdP-Artefakte inkl. CRLs sowie (v) Observability-Indizes (MELT) als Grundlage für korrelierte Analysen. Federations-Profile, Mapping-Schemata und HIL-Policies werden in einer höher geschützten Domäne mitgeführt und nur referenziert. Die Abdeckung richtet sich nach Schutzbedarf und Retention-Klasse; Katalogeinträge dokumentieren Klassifizierung, Versionen, Prüfsummen und Aufbewahrungsfristen.

Strategie und Konsistenzmodell. Backups erfolgen versioniert und verschlüsselt; AAR-/Audit-Ablagen sind immutabel (WORM). Für laufzeitgebundene Komponenten wird Anwendungs-Konsistenz durch Pre-/Post-Hooks (Quiesce/Flush) hergestellt. Architektur-spezifisch gilt:

- A (VM-zentriert): Image- und hypervisorbasierte Snapshots (inkl. Guest-Quiesce) für Management-, Observability- und Übungs-VMs; gezielte Dateisicherungen für Repos und Mirror-Indizes. Netz- und VRF/VLAN-Zustände werden über IaC-Artefakte wiederhergestellt, nicht aus Live-Geräte-Dumps.
- B (Kubernetes): Control-Plane-Sicherungen (etcd Snapshots), objekt- und PV-basierte Backups (z. B. mittels Velero/Restic), plus Export der GitOps-Quellen. Admission-/Mesh-Policies werden als Bundles versioniert und gemeinsam mit Cluster-States gesichert, jedoch strikt getrennt von Laufzeitgeheimnissen.

Katalogisierung und Nachweis. Jede Sicherung erhält einen Backup-Katalogeintrag mit Inhaltsverzeichnis (Artefakt-Typen, Version/Schema-IDs), Kanon der Prüfsummen/Signaturen, Schutzklasse, Retention und Herkunft (Zeitquelle, Ersteller:in). Für Zeitkonsistenz sind alle Stempel UTC-basiert und auf eine lokale Stratum-Quelle referenziert; dadurch bleibt die



Kausalordnung von Run-Ereignissen, Telemetrie und Orchestrierungs-Befehlen auch nach Rehydrierung nachvollziehbar.

Restore-Verfahren. Wiederherstellungen folgen einem abhängigkeitsbewussten Ablauf mit minimalem Seiteneffekt-Risiko: (1) Auswahl eines Recovery-Points gemäß RPO-Ziel und Szenariobezug (Run/Namespace/VM-Gruppe), (2) Isolierte Validierung der Sicherung (Signaturen, Hashes, Schema-/Policy-Kohärenz) in einem Test-Segment, (3) geordnetes Einspielen in die Produktionsumgebung mit Priorisierung von Vertrauensankern (Zeitquelle, PKI/IdP, Registry/Mirror) vor Orchestrierung und Workloads, (4) Integritäts- und Funktionstests (Health, Reachability-Matrix, Query-SLOs) und (5) Freigabe durch Vier-Augen-Prinzip. Teilsicherungen (z. B. einzelner Namespaces bzw. Szenario-Repos) sind dem Full-Restore vorzuziehen, wenn sie die Zielstellung erfüllen und die Kausalität bewahren.

Prüfung und Übungen. Die Wirksamkeit wird über regelmäßige Restore-Proben belegt: stichprobenartig für einzelne Domänen (Repes, Registry, Orchestrierungs-State, Observability-Index) und periodisch als End-to-End-Übung. Prüfungen umfassen (a) Integritätschecks (Hash/Signatur-Vergleich), (b) Schema-/Policy-Validierung der rehydrierten Objekte, (c) Zeitdisziplin (Drift gegenüber Stratum-Quelle) sowie (d) Funktionsnachweise (Provisionierung/Orchestrierung/AAR-Export im Test-Segment). Ergebnisse werden signiert, versioniert und als Evidenz archiviert; Abweichungen fließen in ADRs und Anpassungen der Sicherungsfrequenzen ein.

Sicherheit und Betriebstrennung. Sicherungen sind at-rest und in-transit verschlüsselt; Schlüsselmaterial verbleibt in der Tresorumgebung (HSM/TPM) und wird über Schwellen-Verfahren (z. B. Shamir) verwaltet. Segregation of Duties trennt Erstellung, Transport, Lagerung und Restore-Freigabe. Für Air-Gap-Standorte erfolgt Medienumschlag physisch kontrolliert mit Chain-of-Custody-Protokoll; Retention und Legal-Hold sind technisch erzwungen, die End-of-Life-Behandlung (sichere Vernichtung) dokumentiert.

Akzeptanzkriterien. Ein Backup/Restore-Regime gilt als hinreichend, wenn (i) der definierte RPO/RTO-Korridor eingehalten wird, (ii) jede Sicherung integritäts- und signaturgeprüft rehydriert werden kann, (iii) die Korrelationsfähigkeit von Run-Ereignissen und Telemetrie nach Restore erhalten bleibt und (iv) AAR-/Audit-Ablagen immutabel sowie referenziell vollständig sind. Damit wird die Voraussetzung geschaffen, kritische Zustände kontrolliert wiederherzustellen—ohne Verlust der Beweisqualität und ohne Verstoß gegen die Air-Gap-Prämissen.

4.10.2 Offline-Prozesse

Offline-Prozesse sind für den Betrieb der Trainingsplattform unter hochsicheren und vorzugsweise internetentkoppelten Rahmenbedingungen von zentraler Bedeutung. Sie regeln jene Abläufe, die auch ohne externe Konnektivität verlässlich, nachvollziehbar und sicher durchgeführt werden müssen. Im Mittelpunkt stehen dabei insbesondere die kontrollierte Bereitstellung von Artefakten, Konfigurationen und kryptographischem Material sowie die Sicherstellung von Integrität, Nachvollziehbarkeit und regelkonformer Freigabe. Offline-Prozesse sind damit nicht nur betriebliche Unterstützungsmechanismen, sondern sicherheitskritische Kernprozesse eines belastbaren Air-Gap-Betriebs.

4.10.2.1 Artefakt-Transport (Air-Gap)

Der Air-Gap-Transport stellt die sichere und nachvollziehbare Versorgung der Plattform mit Software-Artefakten (Images, Packages, Signatur, ...) ohne Internetanbindung sicher. Ziel ist ein prüfbarer, manipulationsresistenter Zuführungsprozess, der Integrität und Provenienz nachweist, Schadcode zuverlässig ausschließt und nur policy-konforme Inhalte in die Produktionsdomäne

überführt. Der Prozess ist streng gestuft, arbeitet fail-closed und erzeugt in jeder Phase revisionssichere Evidenz.

Prozessmodell und Zonen. Der Transport folgt einem stufigen Pfad: Physische Übergabe → Quarantäne → Staging → Produktion (WORM).

- Physische Übergabe. Artefakte werden auf versiegelten Datenträgern mit Seriennummern und Transportprotokoll übergeben. Die Versiegelung ist fälschungssicher (Tamper-Evident); Brüche oder Unregelmäßigkeiten führen unmittelbar zur Zurückweisung.
- Quarantäne-Zone. In einer isolierten Umgebung werden Artefaktbündel entpackt und einer mehrstufigen Prüfung unterzogen: (i) Signatur- und Hash-Validierung (z. B. Ed25519/RSA-Signaturen, sha256-Digests) gegen mitgelieferte, signierte Manifestlisten; (ii) SBOM-Kohärenz und Vergleich mit erwarteten Komponenten; (iii) Offline-Malware-Scans und Heuristiken mit lokal gepflegten Virendefinitionen sowie (iv) Schema-/Policy-Checks. Ergebnis ist ein Quarantäne-Bericht mit Prüfkatalog-ID, Prüfsummen, Zeitstempeln (lokale Stratum-Quelle) und Befund.
- Staging. Nur vollständig konforme Bündel werden in ein Staging-Mirror überführt. Dort erfolgen Funktionsproben mit Referenzhardware bzw. -clustern (Smoke-Tests, Minimal-Deployments) und stichprobenartige Rebuild-Überprüfungen.
- Produktion. Nach dokumentierter Freigabe werden Artefakte in unveränderliche Speicherklassen (WORM-Buckets/-Tiers) promotet. Überschreiben ist ausgeschlossen; Updates entstehen ausschließlich als neue Versionen mit eigenem Digest.

Evidenzführung und Nachvollziehbarkeit. Jede Transport- und Prüfphase erzeugt Chain-of-Custody-Belege: Übergabeprotokolle (Person, Zeit, Medium, Siegelstatus), Prüfsummenlisten, Signatur, Quarantäne- und Staging-Entscheide sowie der Freigabevermerk mit Rollenangabe. Zeitstempel basieren konsistent auf der lokalen UTC-Quelle; sämtliche Belege werden signiert und archiviert. Dadurch bleibt die Herkunft jedes Artefakts, einschließlich der verwendeten Prüfkataloge, über den gesamten Lebenszyklus hinweg überprüfbar. Rollen, Pflichten und Trennung der Verantwortlichkeiten. Der Betrieb trennt Transport, Prüfung und Freigabe organisatorisch: Ein Supply-Custodian verantwortet den Medienumschlag, die verantwortliche Person führt Quarantäne-Prüfungen durch, und Plattform-Ops entscheidet über Staging/Promotion. Vier-Augen-Freigaben sind für Promotionen verpflichtend; Notfallpfade sind zeitlich eng begrenzt, dual kontrolliert und auditpflichtig. Fail-closed-Durchsetzung. Jede Verletzung, ungültige Signatur, Digest-Mismatch, SBOM-Drift, Malwarefund, Policy-Verstoß, führt deterministisch zu Quarantäne + Alarm. Betroffene Artefakte werden markiert, Ursachen klassifiziert und nur nach erfolgreicher Neuprüfung erneut betrachtet. Teilfreigaben sind zulässig, wenn Bündel granular signiert sind; ansonsten wird das Gesamtpaket abgelehnt. Datenformate und Bündelung. Für den Air-Gap-Transport werden selbstbeschreibende Bündel empfohlen, die neben den Nutzlasten stets Signaturdateien, SBOMs, Policy-Manifeste, Prüfsummenlisten und einen Transport-Index enthalten. Der Index referenziert alle Bestandteile über unverwechselbare Bezeichner (Digest/Version) und erleichtert die deterministische Wiederherstellung der Prüfsituation. Optional werden Prüfergebnisse als signierte attestations beigefügt, um Prüfketten bei Folgepromotionen zu verkürzen. Metriken und Qualitätsnachweise. Der Prozess wird anhand von Kennzahlen geführt: Lead-Time Quarantäne→Staging/Produktion, Ablehnungsquote nach Befundklassen (Signatur/SBOM/Malware/Policy), Wiederholrate identischer Befunde, Fehlalarmrate (False Positives) sowie Abdeckungsgrad der Prüfregeln je Artefakttyp. Schwellenwerte sind als Policies-as-Code hinterlegt; Über-/Unterschreitungen lösen Maßnahmen (z. B. strengere Staging-Proben, Lieferanten-Feedback) aus. Sonderfälle und Entsorgung. Für Sicherheits-Dringlichkeiten kann ein Emergency Patch Window definiert werden: Die Reihenfolge bleibt stufig, aber Staging-Tests werden verdichtet; zusätzlich gilt eine verkürzte Retentionsfrist für

Telemetrie zur Nachbeobachtung. Nicht benötigte oder kompromittierte Medien werden nach dokumentierten Verfahren datenschutzkonform entsorgt; Entsorgungsnachweise schließen Seriennummern und Vernichtungsmethodik ein. Damit gewährleistet der Artefakt-Transport einen prüfbar, reproduzierbar und manipulationsresistenten Zufluss in der Air-Gap-Umgebung: Nur vollständig verifizierte Artefakte erreichen Produktion; jede Abweichung führt fail-closed zur Quarantäne—mit lückenloser Evidenz für Audit und AAR.

4.10.2.2 Patch-Fenster

Patch-Fenster sind geplante Wartungsperioden, in denen Veränderungen an Plattform, Laufzeitumgebung und Trainingsartefakten kontrolliert, risikobasiert und mit Rückrollgarantie umgesetzt werden. Ziel ist es, die Trainingsdurchführung nicht zu beeinträchtigen, Sicherheitslücken zügig zu schließen und gleichzeitig die Nachweisfähigkeit von Änderungen zu sichern.

Im Vorfeld wird jede Änderung einer Risikoklassifizierung unterzogen (kritisch/hoch/mittel/niedrig). Kritische Sicherheitsbehebungen erhalten Priorität und können in ein außerordentliches Sicherheitsfenster fallen; alle übrigen Maßnahmen werden zu Bündeln zusammengefasst, um Frequenz und Koordinationsaufwand zu minimieren. Jedes Bündel besitzt einen eindeutig referenzierbaren Änderungsantrag mit Umfang, Abhängigkeiten, messbaren Erfolgs-/Abbruchkriterien, geplanter Dauer und betroffenen Zonen/Komponenten. Die zeitliche Kapselung erfolgt in Wartungsslots außerhalb der Haupttrainingszeiten; parallele Übungen werden, sofern möglich, logisch separiert oder vorab auf „read-only“ gestellt. Die Durchführung folgt einem stufenweisen Rollout mit klar definierten Umschaltpunkten. In VM-zentrierter Architektur A werden Snapshots/Clones als Rückkehrpunkt erstellt; Umschaltungen erfolgen host- oder serviceweise. In Cloud-nativer Architektur B werden Revisions/ReplicaSets vorbereitet; Umschaltungen erfolgen per Blue/Green- oder Canary-Muster mit begrenzter Exposition und automatischer Health-Gate-Überwachung. In beiden Architekturen gilt: Bei Nichterreichen vordefinierter Schwellenwerte (z. B. Fehlerraten, Latenzen, Ressourcenbudget) wird der Rollout automatisch abgebrochen und ein Rollback initiiert; der Zustand vor Beginn ist deterministisch wiederherstellbar.

Vor jedem Rollout sind Vorabtests verpflichtend und evidenzgestützt:

1. Funktionalität – End-to-End-Proben des Bereitstellungspfads (Provisionierung, Registrierungen, Start/Stop/Eskalation) und der relevanten Schnittstellen;
2. Sicherheit – statische und laufzeitnahe Policies-as-Code-Prüfungen inklusive Signatur-/SBOM-Verifikation, Admission/Mesh-Regeln (B) bzw. Host/Gateway-Regeln (A);
3. Leistung – Messläufe für Time-to-Train, Orchestrierungs-Latenz (P95) und Observability-Query-SLOs. Nur bei bestandenen Vorabtests wird die Maßnahme für das Patch-Fenster freigegeben.

Während des Fensters laufen Telemetrie-Wächter (synthetische Checks, Liveness/Readiness, Query-SLO-Monitoring) und ein Change-Journal mit UTC-Zeitstempeln aus lokaler Quelle. Jede Teilmaßnahme erzeugt signierte Ereignisse (Start, Umschaltpunkt, Ergebnis) und—bei trainingsrelevantem Bezug—eine AAR-Notiz. Bei Abweichungen gelten vordefinierte Abbruchkriterien: Anstieg der Fehlerrate über Schwelle, Verletzung eines SLO, Policy-Verstoß oder Integritätsfehler. Abbrüche sind fail-closed auszuführen, einschließlich Isolationsmaßnahmen, Entkopplung externer Strecken (Föderation) und Rückkehr auf den letzten freigegebenen Stand. Die Kommunikation ist rollenspezifisch strukturiert: Vorabankündigung des Fensters mit Umfang und erwarteter Wirkung; Live-Statusmeldungen bei Umschaltpunkten; Abschlussbericht mit erreichten Kennzahlen, aufgetretenen Abweichungen und ggf. Rückrollbegründung. Für Ausnahmen (z. B. kritische Sicherheitslücke) existiert ein komprimierter Notfallpfad mit verkürzten,

aber nicht entfallenen Prüfungen und zwingender Vier-Augen-Freigabe. Erfolgskriterien eines Patch-Fensters sind (i) Null ungeplante Trainingsunterbrechungen, (ii) Bestandene Vorabtests mit dokumentierten Ergebnissen, (iii) keine SLO-Verletzungen während und nach dem Rollout, (iv) Rollback-Fähigkeit nachweislich vorhanden (Probe oder Dry-Run) und (v) vollständige Evidenz (Signaturen, SBOM-Bezüge, Change-Journal, AAR-Referenzen). Metriken zur Steuerung umfassen die Change-Fehlerrate, Mean Time to Detect Abweichungen, Anteil automatisierter Rückrollvorgänge, Dauer und Lead-Time pro Bündel sowie die kumulierte Trainingszeit, die unter Policy-bedingter Einschränkung stand. Abweichungen führen zu Lessons Learned und dokumentierten Anpassungen der Bündelungs-, Test- und Umschaltstrategie.

4.10.2.3 Schlüsselrotation

Die Schlüsselrotation minimiert die kryptographische Exposition der Plattform und erhält zugleich die Vertrauenskette ohne Betriebsunterbrechung. Sie umfasst alle Vertrauensdomänen der Lösung—Identitätsprovider/PKI, Föderations-Strecken, Service-Mesh/Workload-Identitäten sowie signierende Systemdienste—und ist für den Air-Gap-Betrieb so auszulegen, dass Ausgabe, Verteilung und Widerruf ausschließlich über lokale Vertriebswege erfolgen.

Planung. Ausgangspunkt ist ein rotationsfähiges Inventar sämtlicher Schlüssel- und Zertifikatsobjekte einschließlich Ketten (Root/Intermediate/Leaf), Gültigkeiten, Kryptoprofile und Abhängigkeiten. Auf dieser Basis werden ein Rotationskalender und TTL-Ziele definiert: kurze Gültigkeiten für Laufzeit-Identitäten (z. B. SVIDs im Stundenbereich), moderat längere für Server-/Client-Zertifikate und strikt abgeschottete Lebenszyklen für CA-Schlüssel. Der Scope wird je Zyklus festgelegt (IdP/PKI, Föderation, Mesh), inklusive Reihenfolge der Umschaltung (zuerst Trust Anchors bzw. Trust Bundles, dann Intermediates, zuletzt Leaf-Zertifikate). Abhängigkeitsanalysen (z. B. gegenseitige TLS-Prüfungen zwischen Orchestrierung, Portalen, Gateways) und Laborproben mit repräsentativen Topologien dienen der Risikobewertung und Terminierung außerhalb trainingskritischer Phasen.

Durchführung. Schlüsselmaterial wird in einer abgeschotteten Tresorumgebung (HSM/TPM) erzeugt; private Schlüssel verlassen den Schutzbereich nicht im Klartext. Für Architektur A und die IdP-Dienste in B werden CSRs erstellt, signiert und als neue Kette bereitgestellt. In SPIFFE-Domänen (Architektur B) wird zuerst das Trust Bundle veröffentlicht, anschließend die Ausstellung neuer SVIDs mit verkürzter TTL aktiviert. Die Umschaltung erfolgt parallel: Systeme akzeptieren für eine definierte Übergangszeit sowohl alte als auch neue Anker/Zertifikate (Dual-Acceptance), während mTLS-Handshakes aktiv verifiziert werden. Nach Erreichen der Abdeckungsschwelle (z. B. $\geq 99\%$ Endpunkte mit neuem Material) erfolgt die atomare Umschaltung: Alte Zertifikate werden widerrufen, Offline-CRLs bzw. aktualisierte Trust Bundles über die Air-Gap-Mirror verteilt und die Dual-Acceptance beendet. Föderations-Strecken erhalten kurzlebige Schlüsselpaare; der Roll-over wird zwischen den Sites koordiniert, damit Join/Resign-Ereignisse ohne Partial-Trust verbleiben. Für Architektur A werden Host-/Dienstzertifikate auf Gateways und Hypervisor-nahen Diensten in derselben Sequenz migriert; in Architektur B aktualisiert die Control-Plane die Sidecar-Zertifikate kontrolliert pro Namespace, flankiert von Admission-Gates, die nur frische, signierte Identitäten zulassen.

Nachweis und Qualitätssicherung. Jeder Schritt erzeugt Tresor-Journale (Schlüsselereignisse, Seriennummern, Aussteller, Fingerprints), Propagationsmessungen (Zeit bis zur clusterweiten bzw. siteweiten Sichtbarkeit des neuen Materials) und Negativtests (Verbindungsversuche mit abgelaufenen/gesperrten Zertifikaten, die deterministisch scheitern müssen). Stichproben über kritische Kommunikationspfade (Orchestrierung↔Portal, Föderations-Gateway↔Partner, Mesh-Service↔Service) belegen erfolgreiche mTLS-Aushandlungen mit der neuen Kette. Ergebnisse werden signiert, WORM-fähig archiviert und—sofern trainingsrelevant—im AAR referenziert. Akzeptanzkriterien umfassen u. a.: 0 ungeplante Unterbrechungen, 100 % mTLS-Endpunkte mit

neuem Zertifikat innerhalb des definierten Fensters, vollständiger Widerruf des Altmaterials (CRL-Abdeckung) und fehlertolerante Handshakes während der Dual-Acceptance.

Governance und Sonderfälle. Ausgabe, Freigabe und Widerruf unterliegen Segregation of Duties und Vier-Augen-Freigaben; Key-Ceremonies (Erzeugung/Archivierung von CA-Material) sind formal dokumentiert. Für Kompromissfälle existiert ein Notfall-Rollover mit sofortiger Entkopplung betroffener Strecken, erzwungenem Widerruf, beschleunigter Bundle-Verteilung und anschließender Ursachenanalyse. Speicher- und Transportpfade der Artefakte bleiben durchgehend verschlüsselt; Speicherbereiche mit temporären Schlüsseln werden nach Abschluss sicher gelöscht (Zeroization). Abschließend werden Runbooks und Rotationskalender anhand der Messwerte (Propagationszeiten, Fehlerraten, Anteil automatisierter Umschaltungen) angepasst und als ADR versioniert—so bleibt die Schlüsselrotation ein wiederholbares, auditierbares Verfahren, das die kryptographische Angriffsfläche kontinuierlich reduziert, ohne die Betriebsziele der Trainingsplattform zu beeinträchtigen.

4.10.3 SLA/SLOs und Kapazitätsplanung

Die Betriebsfähigkeit der Trainingsplattform hängt nicht allein von ihrer technischen Architektur, sondern ebenso von klar definierten Servicezielen und einer vorausschauenden Kapazitätsplanung ab. SLA/SLOs schaffen dabei einen verbindlichen Rahmen für Verfügbarkeit, Wiederherstellungszeiten, Performance und Betriebsqualität, während die Kapazitätsplanung sicherstellt, dass Trainings, Übungen und Lastspitzen auch unter variierenden Nutzungsbedingungen verlässlich unterstützt werden können. Im militärischen Ausbildungskontext dienen diese Festlegungen somit nicht nur der betrieblichen Steuerung, sondern auch der Absicherung von Planbarkeit, Nachvollziehbarkeit und resilientem Plattformbetrieb.

4.10.3.1 Service Level Objectives (SLOs) und Messmethoden

Dieses Unterkapitel formuliert die Qualitätsziele des Trainingsbetriebs als SLOs und präzisiert deren Messmethodik so, dass Ergebnisse nachvollziehbar, reproduzierbar und zwischen den Architekturen A und B vergleichbar sind. Ein SLO wird als Tupel verstanden: (Messgröße, Zielwert, Beobachtungsfenster, Auswertung). Gemessen wird stets an realen Betriebsereignissen; Auswertungen erfolgen per Perzentile (insb. P95), um Lastspitzen adäquat abzubilden. Geplante Wartungsfenster werden in den Analysen ausgeschlossen, die betrachtete Population (z. B. Run-Typ, Site) wird explizit angegeben, und die Messpunkte sind eindeutig auf Artefakt- und Release-Stände rückführbar.

Time-to-Train (Standard-Range). Ziel: Provisionierung ≤ 30 min. Messung: Ende-zu-Ende-Dauer vom freigegebenen Sollzustand bis zu vollständigen Health-Signalen der Trainingsumgebung. Ausgewertet wird pro Run, reportet als P95 je Kalenderwoche. Der Pfad umfasst alle relevanten Schritte der Bereitstellung; Wartungsfenster sind ausgeschlossen.

Orchestrierungs-Latenz. Ziel: $P95 < 5$ s für Start, Pause und Event-Injection. Messung: Differenz zwischen Kommandosignal und bestätigtem Zustandsübergang; Auswertung getrennt nach Kommandoart, aggregiert per P95 über das Beobachtungsfenster. Koinzidenzen mit Kapazitäts- oder Policy-Ereignissen werden analytisch berücksichtigt.

Lab-Reset (Hands-on). Ziel: ≤ 60 s. Messung: Zeit vom Reset-Trigger im Portal bis zur Rückmeldung „bereit“. Unterschieden wird nach Implementierungspfad (z. B. Snapshot/Clone vs. Neuansatz); Berichterstattung erfolgt getrennt nach Pfad und Lab-Kategorie.

Observability-Query (Standard-Sichten). Ziel: $P95 < 2$ s. Messung: Antwortzeit definierter, kuratierter Abfragen (z. B. Korrelationstimeline, Kernmetriken) im produktiven Betrieb und über

synthetische Checks. Kardinalität und Downsampling sind für Vergleichbarkeit fixiert; Auswertung pro Sicht.

Ingest-Verlustquote. Ziel: $\leq 0,5$ % je Kanal (OTLP, Syslog, NetFlow/IPFIX). Messung: Fehlende Sequenzen/Offsets relativ zur erwarteten Ereignismenge im Zeitfenster; Analyse kanalweise und run-bezogen, um Vermischung paralleler Übungsrunden zu vermeiden.

Verfügbarkeit zentraler Dienste.

Ziel: $\geq 99,5$ % für IdP/PKI, Orchestrierung und Registry/Mirror. Messung: 1–(ungeplante Ausfallzeit/ Gesamtzeit–geplante Wartung) über synthetische Funktionsprüfungen und Betriebsjournale; Ausweisung zonenbezogen (Management, Übung, Föderation).

Compliance-Gates. Ziel: 100 % Konformität (Signatur, SBOM, Schema/Policy); Verstöße werden blockiert. Messung: Anteil erfolgreich passierter Prüfschritte an allen geprüften Artefakten und Deploy-Aktionen; Klassifizierung der Fehlgründe für Trendanalysen.

Föderations-Drift. Ziel: $P95 < 50$ ms (konfigurationsabhängig). Messung: Zeitdifferenz semantisch identischer Ereignisse zwischen föderierten Sites; Grundlage sind dedizierte Drift-Metriken und Protokolle der Kopplungsstrecken, ausgewertet pro Übungslauf.

Methodische Festlegungen.

Auswertefenster: rollierend und kalenderbasiert, mit expliziten Ausschlüssen für genehmigte Wartung; Sonderfenster werden separat berichtet.

Aggregation: primär P95, ergänzt um Median und Fehlerbudget; Ausreißerbehandlung ist dokumentiert.

Stratifizierung: Berichte getrennt nach Run-Typ, Site und Architekturvariante; Vergleichsstudien nur auf basisgleich normierten Sichten.

Rückführbarkeit: Jeder Messpunkt verweist auf den zugehörigen Konfigurations- und Artefaktstand (Versionen, Digests) sowie auf die zugehörigen Betriebsereignisse, sodass Ergebnisse auditfest belegt werden können.

Mit dieser Systematik werden SLOs zu belastbaren Qualitätsgrenzen: Zielwerte sind präzise definiert, Messwege standardisiert und Berichte so strukturiert, dass sie sowohl den laufenden Betrieb steuern als auch Entscheidungen im Variantenvergleich empirisch fundieren.

4.10.3.2 Kapazitätsplanung

Ziel der Kapazitätsplanung ist es, ausreichende Vorhaltekapazität für erwartete Spitzenlasten – insbesondere mehrere parallele Übungsrunden – bereitzustellen und zugleich Noisy-Neighbor-Effekte zuverlässig auszuschließen. Die Planung ist deterministisch ausgelegt: Annahmen, Messwerte und Ableitungen sind dokumentiert, reproduzierbar und architekturübergreifend vergleichbar.

Ressourcenprofil pro Run. Für jedes Szenario wird zunächst ein konservatives Ressourcenprofil ermittelt, das die dominanten Achsen abbildet: Rechenzeit (vCPU), Arbeitsspeicher (RAM), Speicherkapazität und -leistung (Kapazität und IOPS) sowie Netzanforderungen (Durchsatz und – falls relevant – Latenzbudgets). Die Profile basieren auf Messläufen mit Referenzszenarien unter realistischen Bedingungen (z. B. typische Teilnehmerzahl, übliche Telemetriemengen, Standard-Emulationen) und berücksichtigen bereits die Plattform-Overheads durch Virtualisierung bzw. Container-Orchestrierung.

Dimensionierende Achse. Die maximal gleichzeitig betreibbare Zahl an Runs wird durch diejenige Ressourcenachse begrenzt, die als erste ausgeschöpft ist (z. B. vCPU, RAM, IOPS oder Netz). Um kurzfristige Lastspitzen, Messunsicherheiten und Hintergrundaufgaben sicher abzufangen, wird ein Sicherheitszuschlag („Headroom“) eingeplant, der typischerweise zwischen 20 % und 30 % liegt. Zusätzlich fließt ein Effizienzfaktor ein, der die zu erwartenden Verluste durch Scheduling-, Netzwerk- und Storage-Overheads realistisch abbildet. Kapazitätsaussagen werden stets als Bandbreite ausgewiesen (z. B. „8–10 parallele Standard-Runs auf Cluster X“), nicht als Punktwerte.

Architektur-spezifische Leitplanken.

Architektur A (VM-zentriert): Die Plattform skaliert primär vertikal (mehr vCPU/RAM pro VM); horizontale Elastizität ist begrenzt. Snapshot/Clone-Mechanismen beschleunigen zwar Replikation und Reset, erhöhen aber kurzzeitig I/O-Last und Belegungsdruck auf die Storage-Pools. Overcommit wird – wenn überhaupt – nur konservativ eingesetzt, und nur dort, wo die SLOs (Time-to-Train, Orchestrierungs-Latenz) nachweislich nicht gefährdet sind.

Architektur B (Kubernetes): Die Plattform skaliert horizontal über zusätzliche Replikate bzw. Nodes. Quotas und LimitRanges begrenzen Mandanten, Eviction-Policies schützen vor Drosselung kritischer Workloads. Ein moderates Overcommit ist möglich, muss aber gegen P95-SLOs und Abbruchkriterien der Admission-Kontrollen kalibriert sein, um Verdrängungseffekte zu vermeiden.

Planungsprozess. Die Kapazitätsplanung folgt einem vierstufigen Verfahren:

Profilerstellung: Messläufe pro Szenariotyp (Standard, I/O-intensiv, Netz-intensiv) mit Instrumentierung auf MELT-Ebene; Ermittlung belastbarer Verbrauchswerte pro Run und Achse.

Prognose: Ableitung des zu erwartenden Parallelitätsbedarfs aus Terminplänen, Saisonalität (Ausbildungsrhythmen), typischen Klassenstärken und geplanten Föderationsübungen; Szenarien mit erhöhter Kritikalität werden separat geführt.

Kapazitätsbudget: Festlegung von Obergrenzen pro Cluster/Standort unter Einschluss von N+1-Redundanz und Headroom; Definition harter Admission-Regeln, die neue Runs deterministisch ablehnen, wenn Mindestressourcen nicht nachweislich verfügbar sind.

Kalibrierung: Regelmäßiger Abgleich mit realer Auslastung und SLO-Einhaltung; Anpassung der Profile, Headroom-Sätze und Overcommit-Schranken auf Basis empirischer Daten.

Noisy-Neighbor-Prävention. Die Plattform setzt technische Isolationsmechanismen ein, um gegenseitige Beeinflussungen zu verhindern: In A durch VRF/VLAN-Platzierung, Storage-Pool-Zuweisung und Bandbreiten-Shaping auf Gateway-Ebene; in B durch Namespaces, NetworkPolicies, ResourceQuotas sowie – falls notwendig – eigene Storage- und Ingress/Egress-Klassen pro Mandant. Admission-Gates verweigern den Start weiterer Runs, sobald definierte Schwellenwerte überschritten sind.

Kopplung an SLOs. Kapazitätsentscheidungen werden an SLO-Erfüllung rückgekoppelt. Steigen z. B. Orchestrierungs-Latenzen in das P95-Grenzband oder verfehlen Labs den Reset-Zielwert, wird die zulässige Parallelität sofort reduziert oder das betroffene Szenarioprofil angepasst. Umgekehrt können positive Trends (unterausgelastete Achsen, stabile SLO-Reserven) vorsichtige Erhöhungen rechtfertigen.

Prüfung und Evidenz. Vor wesentlichen Anpassungen (z. B. Erhöhung der maximalen Parallelität) sind Last- und Stresstests verpflichtend, die die dimensionierende Achse bewusst ausreizen und SLO-Stabilität belegen. Ergebnisse werden mit UTC-Zeitstempeln aufgezeichnet, in AARs referenziert und als ADR versioniert. Prognosefehler, Admission-Ablehnungen und SLO-Verletzungen fließen in eine kontinuierliche Lessons-Learned-Schleife ein.

Betriebliche Reserve und Degradationspfade. Neben dem Headroom für Lastspitzen wird eine operative Reserve für Wartung, Patches und DR-Rückläufe vorgehalten. Für außergewöhnliche Bedarfe (z. B. föderierte Großübungen) sind Degradationspfade definiert, die nicht-kritische Dienste temporär drosseln oder isolieren, ohne Trainingsziele zu gefährden (z. B. Verzögerung nicht essenzieller Exporte, Reduktion der Dashboard-Kardinalität).

4.10.3.3 Governance & Evidenz

Die Governance dieses Betriebsmodells stellt sicher, dass Qualität, Sicherheit und Air-Gap-Konformität nicht nur als Zielbilder definiert, sondern laufend nachweisbar erreicht werden. Hierzu werden sämtliche Steuerungsdokumente und Prüfergebnisse entlang eines einheitlichen Evidenzprozesses geführt und versioniert. Runbooks, SLO-Definitionen, Kapazitätsannahmen und die Resultate standardisierter Tests (z. B. Disconnect-, Restore- und DR-Drills) werden als Architecture Decision Records (ADRs) mit kryptografischer Signatur und UTC-Zeitstempel abgelegt und in den After-Action-Reports (AARs) referenziert. Damit ist jede operative Entscheidung, einschließlich ihrer Voraussetzungen und Nebenwirkungen, rückführbar auf den zugehörigen Artefakt- und Konfigurationsstand.

Die Auditfähigkeit wird über einen wiederkehrenden Prüfzyklus gesichert, der Wirksamkeit und Reifegrade zentraler Kontrollen beurteilt. Dazu zählen u. a. Policy-Trefferquoten (Anteil blockierter, nicht konformer Vorgänge), Validierungslatenzen in den Gate-Stufen, Query-SLOs der Observability-Sichten sowie Föderations-Belege (Handshake-Evidenz, Zeitdrift-Messungen, Mapping-Protokolle). Alle Audit-Artefakte werden manipulationsresistent in WORM-Speichern aufbewahrt; Schutzklassen und Aufbewahrungsfristen folgen dem im Sicherheitskapitel verankerten Datenregime. Für interne und externe Prüfungen ist ein Minimal-Export der Belege vorgesehen, der die Verifikation erlaubt, ohne hochschutzbedürftige Details preiszugeben.

Abweichungen vom Sollzustand werden technisch erzwungen behandelt. Überschreiten Metriken definierte Schwellen oder verletzen Artefakte Signatur-, SBOM- oder Schema-Vorgaben, greift das automatische Gating: betroffene Änderungen oder Laufzeiten werden in Quarantäne versetzt, zurückgerollt oder – bei intersite-Kopplungen – entkoppelt. Jede Abweichung löst einen Post-Event-Review mit dokumentierter Ursachenanalyse aus; daraus resultierende Corrective and Preventive Actions (CAPA) werden terminiert, priorisiert (Risiko- und Trainingsrelevanz) und als ADR nachgeführt. Wirksamkeitskontrollen stellen sicher, dass getroffene Maßnahmen nachhaltig greifen; verbleibende Restrisiken werden bewertet und – sofern erforderlich – im Risikoportfolio des Projekts nachgeführt.

Die organisatorische Absicherung erfolgt über Rollen- und Freigaberegeln mit strikter Aufgabentrennung: Betrieb (Plattform-Ops), Sicherheit/Governance und Übungsleitung genehmigen und dokumentieren Entscheidungen innerhalb ihres Mandats; für netz-, schlüssel- und lieferkettenrelevante Vorgänge gilt das Vier-Augen-Prinzip. Ein konsistenter Belegfluss (ADRs → Pipelines/Gates → AAR-Referenzen → Audit-Ablage) schließt die Chain-of-Custody und ermöglicht aussagekräftige Trendanalysen – etwa zur Entwicklung der Fehlerraten, der Mean-Time-to-Detect/Remediate oder der SLO-Konformität unter Last.

4.11 Validierung & Nachweisführung

Validierung und Nachweisführung werden in diesem Bericht als empirischer, hypothesengeleiteter Prozess verstanden. Aus den normativen Muss-/Soll-Vorgaben werden zunächst prüfbare Hypothesen abgeleitet und als maschinenlesbare Testobjekte operationalisiert. Jedes Testobjekt umfasst den definierten Eingaberaum (inklusive Grenz- und Fehlerszenarien), den Prüfpfad über beteiligte Schnittstellen und Zonen, die erwarteten Effekte auf Systemzustände, präzise Messpunkte mit UTC-Referenz sowie die vorgesehene Evidenzform (z. B. signierte Logzeilen, Digest-Listen, AAR-Auszüge). Diese Spezifikation wird versioniert und signiert, sodass Reproduzierbarkeit und Nachvollziehbarkeit über alle Iterationen gewährleistet sind und sich Befunde deterministisch auf Artefakt- und Release-Stände zurückführen lassen.

Die Versuchsführung folgt Prinzipien, Instrumentierung, Zeitbasis und Korrelationsschlüssel (run_id) werden vorab festgelegt, Störgrößen werden durch Wiederholungsmessungen, kontrollierte Startbedingungen und getrennte Auswertungskohorten adressiert. Interne Validität wird durch fail-closed-Gates und idempotente Rollback-Pfade abgesichert; externe Validität entsteht durch die Nutzung kuratierter Lastprofile und repräsentativer Föderations- und HIL-Topologien. Die Ergebnisdarstellung erfolgt per Perzentilen anstelle von Mittelwerten, um Lastspitzen angemessen zu erfassen; genehmigte Wartungsfenster sind explizit ausgeschlossen. Hochschutzbedürftige Belege werden nicht eingebettet, sondern über Hash-/Signatur-Referenzen attestiert; die vollständige Belegkette wird WORM-fähig archiviert. Die Priorisierung der Prüfkampagnen ist risikobasiert und richtet sich nach Auswirkungs- und Eintrittswahrscheinlichkeit. Lieferkette, Air-Gap-Robustheit, Schlüssel- und Identitätsmanagement, Föderationsisolation sowie HIL-Guards erhalten Vorrang; Leistungs- und Skalierungsnachweise fokussieren die dimensionierende Ressourcenachse (CPU, RAM, IOPS, Netz), ohne Noisy-Neighbor-Effekte zu induzieren. Für jede Kampagne sind Abbruchkriterien und zulässige Schwankungsbänder vorab definiert; Verletzungen führen deterministisch zu Quarantäne, Rollback oder Entkopplung betroffener Strecken. Abweichungen werden im Rahmen strukturierter Post-Event-Analysen in Ursachen (Konfiguration, Kapazität, Implementierung, Datenqualität) zerlegt, Korrektur-/Präventionsmaßnahmen (CAPA) terminlich fixiert und ihre Wirksamkeit in Folgeläufen überprüft.

Die Abnahme stützt sich auf objektive, vorab festgelegte Schwellenwerte und ist rollengebunden organisiert. Anstelle redundanter Wiederholung bereits definierter Zielgrößen liegt der Schwerpunkt dieses Kapitels auf der Messdisziplin, der Festlegung zulässiger Ausnahmen, der Stratifizierung der Auswertung und der Sicherung der Chain-of-Custody. Entscheidungen werden in signierten ADRs dokumentiert und mit den relevanten AAR-Referenzen, Artefakt-Digests und Schema-IDs verknüpft. Dadurch wird nicht lediglich das Bestehen einzelner Tests konstatiert, sondern die Beherrschung der zugrunde liegenden Mechanismen belegt: deterministische Bereitstellung, reproduzierbarer Betrieb, policy-konforme Interoperabilität und auditfeste Evidenz.

Schließlich wird der Übergang von der Konzept- zur Einsatzreife als Sequenz kontrollierter Experimente gestaltet. Der PoC-/MVP-Fahrplan reduziert in aufeinanderfolgenden Iterationen gezielt Unsicherheit entlang der kritischsten Hypothesen (z. B. Reset-Zeitfenster, Föderations-Drift, Disconnect-Resilienz) und erzeugt dabei fortlaufend qualifizierte Evidenz. Jede Stufe besitzt klar definierte Entry-/Exit-Kriterien, liefert signierte Zwischen-AARs sowie aktualisierte ADRs und erlaubt bei Regressionen den geordneten Rücksprung. Validierung und Nachweisführung werden so zu einem integralen Bestandteil der Governance: normativ definierte Anforderungen werden maschinenlesbar, experimentell überprüft, evidenzbasiert entschieden und dauerhaft überprüfbar gehalten.

4.11.1 Zielbild und Vorgehensmodell

Dieses Kapitel definiert Validierung als empirisch fundiertes Nachweisverfahren, dessen Ziel über das bloße Bestehen einzelner Tests hinausgeht. Gefordert ist der belastbare Beleg, dass die Plattform unter den spezifizierten Randbedingungen, einschließlich Air-Gap-Betrieb und föderierten Einsatzlagen, deterministisch bereitgestellt, reproduzierbar betrieben und auditfest dokumentiert werden kann. Das angestrebte Ergebnis ist eine geschlossene Evidenzkette, in der funktionale Korrektheit, Interoperabilität, Leistungsfähigkeit und Sicherheitsdurchsetzung messbar und rückführbar nachgewiesen sind.

Methodisch folgt das Vorgehen einem dreistufigen Prozess:

1. **Ableitung von Prüfobjekten (Traceability):** Muss-/Soll-Anforderungen werden in maschinenlesbare Testobjekte überführt. Jedes Testobjekt spezifiziert Eingaberaum (einschließlich Grenz- und Fehlerszenarien), beteiligte Schnittstellen und Zonen, erwartete Systemeffekte, eindeutig bezeichnete Messpunkte sowie die vorgesehene Evidenzform (z. B. signierte Protokolle, Artefakt-Digests, AAR-Referenzen). Die Spezifikation ist versioniert und signiert, um eine deterministische Rückführung auf Artefakt- und Release-Stände sicherzustellen.
2. **Planung und kontrollierte Durchführung:** Testreihen werden in einer definiert instrumentierten Umgebung ausgeführt. Zeitstempel sind UTC-synchron (lokale Stratum-Quelle), alle Messereignisse werden run-gebunden über die run_id korreliert. Reproduzierbarkeit wird durch konstante Startbedingungen, Wiederholungsläufe und kohortierte Auswertung (Run-Typ, Site, Architekturvariante) abgesichert; Störgrößen (z. B. Hintergrundlast) werden kontrolliert oder analytisch isoliert.
3. **Nachweisführung und Abnahme:** Ergebnisse werden als prüfbare Evidenzartefakte erhoben (Signaturen, Hash-Werte, Schema-IDs, AAR/ADR-Verweise) und gegen objektiv definierte Schwellenwerte beurteilt (SLO-Grenzen, Compliance-Gates). Die Abnahme erfolgt rollenbasiert mit Vier-Augen-Freigabe; Entscheidungen sind eindeutig auf Messpunkte und Artefaktstände rückführbar.

Die Messdisziplin ist verbindlich normiert: Alle Zeit- und Zustandsinformationen nutzen eine konsistente UTC-Basis; Korrelationsschlüssel (run_id) werden konsequent durchgängig verwendet. Hochschutzbedürftige Belege (z. B. Föderations- oder Schlüssel-Nachweise) werden aus Sicherheitsgründen nicht eingebettet, sondern ausschließlich über Hash-/Signatur-Referenzen attestiert. Primärdaten, Protokolle und Testberichte werden WORM-fähig archiviert, um Unveränderlichkeit und langfristige Prüfbarkeit zu gewährleisten. Die Güte der Validierung wird über interne und externe Validität adressiert. Interne Validität entsteht durch fail-closed-Durchsetzung (Schema-, Signatur-, Policy-Gates), idempotente Rollback-Pfade und deterministische Orchestrierungsbestätigungen. Externe Validität wird durch repräsentative Last- und Topologieprofile (einschließlich federierter Kopplungen und HIL-Pfade) und durch die getrennte Berichterstattung nach Kohorten sichergestellt. Abweichungen führen deterministisch zu Quarantäne, Rollback oder Entkopplung und werden im Rahmen strukturierter Post-Event-Analysen in CAPA-Maßnahmen (Corrective/Preventive Actions) überführt, deren Wirksamkeit in Folgeläufen nachgewiesen wird.

4.11.2 Testplan: Funktions-, Integrations-, Last-, Sicherheits- und Föderationstests

Der Testplan operationalisiert die Validierung durch klar abgegrenzte Prüfdisziplinen. Jede Disziplin formuliert Prüfthesen, definiert Versuchsaufbau und Messinstrumente, benennt Messgrößen mit Akzeptanzschwellen und erzeugt prüfbare Evidenzartefakte. Alle Verfahren

arbeiten deterministisch, run-gebunden und mit konsistenter Zeitbasis; Hochschutz-Belege werden ausschließlich referenziert.

4.11.2.1 Funktionstests

Ziel & Prüfthesen. Einzelkomponenten erfüllen ihre spezifizierten Verhaltensverträge. Typische Thesen: „Szenarioobjekte sind nach Anlage vollständig versioniert und signiert“, „Orchestrierungsbefehle führen zu exakt einem Zustandsübergang“, „AAR-Erzeugung liefert ein signiertes Manifest mit konsistenten Referenzen“.

Versuchsaufbau. Minimalistische Referenzumgebung, synthetische Inputs (Valid/Invalid), deterministische Startzustände (z. B. leerer Katalog, definierter Ressourcenpool). Instrumentierung auf API-Ebene (Request/Response-Tracing), Event-Bus-Tapping, sowie strukturierte Fehlerkanäle.

Prüfschritte (Auswahl).

- Szenario-Lebenszyklus: Anlegen → Parser/Validator → Signatur/Hash → Vier-Augen-Freigabe → Katalogsicht.
- Orchestrierung: Start/Pause/Resume/Eskalation mit idempotenten Kommandos; Bestätigungen nur nach erreichtem Quorum.
- Hands-on-Funktionen: Reset/Replay, Scoring-Ereignisse, Bindung an Run-Kontext.
- AAR-Pipeline: Aggregation → Manifest → Signatur → Export.
- HIL-Registrierung: Aufnahme, Policy-Zuordnung, Rate-Limit-Durchsetzung.

Messgrößen & Akzeptanz. Fehlerrückgabe mit präziser Fundstelle; kein Partial-State nach Abbruch; deterministische Wiederholbarkeit (≥3 identische Läufe); vollständige Protokollierung der kritischen Pfade.

Negativpfade. Ungültige Schemen, fehlende Signaturen, Ressourcenkonflikte, doppelte Kommandos; erwartetes Verhalten: fail-closed, konsistenter Rollback, eindeutige Diagnose.

Evidenz. Signierte API-Traces, Validator-Reports, Artefakt-Digests, AAR-Manifestauszüge (nur Referenzen auf hochschützenswerte Inhalte).

4.11.2.2 Integrationstests

Ziel & Prüfthesen. End-to-End-Ketten liefern konsistente, korrelierbare Ergebnisse über Systemgrenzen. Thesen: „IaC-Provisionierung resultiert in orchestrierbaren Ressourcen“, „Ingest-Daten erscheinen korrekt korreliert in Standard-Sichten“, „Supply-Chain-Pfad erzwingt Signatur/SBOM ohne Umgehung“.

Versuchsaufbau. Realistische Kette von Quell- bis Zielsystem (z. B. Quarantäne → Staging → Produktion; IaC → Orchestrierung → Observability → AAR). Einheitliche Run-IDs und Schema-IDs, definierte Testdaten (synthetisch/kuratierte Mitschnitte).

Prüfpfade (Auswahl).

- IaC → Orchestrierung: Plan/Apply → Health-Checks → Run-Registrierung.
- Ingest → Dashboard: OTLP/Syslog/NetFlow → Korrelation → Query-Sichten.
- Artefakt-Supply: Import → Prüfung → Promotion (WORM).
- Identität/RBAC: OIDC/SAML-Flüsse, Rollenprüfungen an kritischen Operationen.

- Simulation ↔ Portal: Ereignisweitergabe, Scoring-Kopplung, Fehlerpropagierung.

Messgrößen & Akzeptanz. Lückenlose Ereigniskette (keine Drops/Duplikate), eindeutige Korrelation, konsistente Schemen, determinierte Fehlerpropagierung; keine unautorisierten Datenflüsse zwischen Zonen.

Negativpfade. Schema-Drift, fehlende Signatur, Token-Ablauf, Ressourcenermangelung; erwartetes Verhalten: Blockade mit strukturiertem Befund.

Evidenz. End-to-End-Traces, Mapping-Nachweise, Build/Deploy-Provenienz, Gate-Entscheide (signiert).

4.11.2.3 Last- und Leistungstests

Ziel & Prüfthesen. SLO-Zielwerte werden unter realistischer Parallelität eingehalten; dimensionierende Achsen sind identifiziert. Thesen: „Time-to-Train bleibt unter Zielschwelle bei n parallelen Standard-Ranges“, „Reset-Stürme unterschreiten das 60-Sekunden-Ziel“, „Query-Sichten erfüllen P95-Vorgaben“.

Versuchsdesign.

- Workload-Modelle: Stufenlast (Ramp-Up), Burst-Profil (Reset-Sturm), Soak-Tests (Dauerlast).
- Isolation: Admissionschranken aktiv; keine Beeinflussung paralleler Trainings (Noisy-Neighbor-Prävention).
- Messung: Ende-zu-Ende-Marker, P-Perzentile, Fehlerbudget-Tracking; Profilierung entlang CPU/RAM/IOPS/Netz.
- Szenarien (Beispiele).
- Gleichzeitige Provisionierung mehrerer Übungen.
- Orchestrierte Event-Wellen (Start/Pause/Event-Injection) mit definierten Intervallen.
- Abfrage-Spitzen in Observability-Sichten bei wachsender Datenkardinalität.

Akzeptanz. Einhaltung der Zielwerte über das Beobachtungsfenster, stabiler Betrieb (keine Evictions/Throttling auf kritischen Diensten), reproduzierbare Ergebnisse bei Wiederholungsläufen.

Evidenz. Laufzeitprofile, Kapazitätsnutzung je Achse, SLO-Reports, Admission-Entscheide, AAR-Referenzen auf Messreihen.

4.11.2.4 Sicherheitstests

Ziel & Prüfthesen. Sicherheitskontrollen sind wirksam, nicht umgehbar und auditierbar. Thesen: „Air-Gap hält über den definierten Zeitraum ohne externe Abhängigkeiten“, „Lieferketten-Gates verhindern unsignierte/abweichende Artefakte“, „Schlüsselrotation verläuft ohne Unterbrechung und mit vollständigem Widerruf“.

Prüffelder.

- Air-Gap-Nachweis: Disconnect-Drill mit Telemetrie auf unerlaubte Egress-Versuche; Logs ohne externe Requests.
- Supply-Chain: Signatur/SBOM-Pflicht, Quarantäne-Import, WORM-Promotion.

- Härting: Baseline-Benchmarks (OS/Container), „Default-Deny“ an Zonenrändern, Mikrosegmentierung.
- Schlüsselmanagement: Dual-Acceptance, atomare Umschaltung, Offline-CRLs/Trust-Bundles, Negativtests (abgelaufene/gesperrte Zertifikate).
- Incident-Response: Erstdiagnosepfade, Isolationsmaßnahmen, forensische Sicherung, AAR-Dokumentation.

Akzeptanz. Durchgängig fail-closed: Verstöße führen deterministisch zu Quarantäne/Rollback/Entkopplung; vollständige Belege der Kontrollen (Signaturen, Hashes, Policies-Treffer, Widerrufslisten).

Evidenz. Disconnect-Protokolle, Gate-Berichte, Härtingnachweise, Rotations-Journale, Forensik-Metadaten (nur Referenzen, keine Geheimnisse).

4.11.2.5 Föderationstests

Ziel & Prüfthesen. Inter-Site-Kopplungen sind sicher, minimal-exponiert und zeitlich konsistent. Thesen: „Handshake-Evidenz ist vollständig“, „DDS↔HLA-Mapping ist schema-/QoS-konform“, „Timeline-Drift bleibt im zulässigen Korridor“, „Isolierung zwischen Mandanten/Sites ist lückenlos“.

Versuchsaufbau. Zwei oder mehr Sites mit dedizierten Föderations-Strecken (VRF/VPN), kurzlebigen Schlüsseln, getrennten Namensräumen. Synthetic Topics/Objekte und kuratierte Real-Ereignisse als Prüfgrundlage.

Prüfschritte.

- Trust Establishment: Zertifikatsketten, Federation-Agreement, Key-Rotation synchronisiert.
- Mapping-Validierung: DDS-Topics ↔ HLA-Objekte/Interaktionen mit Schema-/QoS-Checks; Negativtests bei Inkompatibilitäten.
- Isolationsnachweis: Kein Cross-Tenant-Zugriff, Export-Sichten strikt minimal.
- Zeitkonsistenz: Drift-Messung entlang der Strecke; Kennzeichnung im AAR bei Grenznähe.

Akzeptanz. Vollständiger Proof-of-Federation (signiert), dokumentierte Drift innerhalb Toleranz, keine Policy-Verstöße, deterministische Entkopplung im Fehlerfall.

Evidenz. Handshake-Protokolle, Mapping-Reports, Drift-Zeitreihen, Export-/Import-Manifeste, AAR-Referenzen.

4.11.3 Abnahmekriterien je Anforderung

Die Abnahme erfolgt nach einem einheitlichen, evidenzbasierten Schema, das für jede Anforderung—funktional wie nicht-funktional—präzise festlegt, welcher Messpunkt beobachtet wird, welcher Schwellenwert als erfüllt gilt und in welcher Evidenzform der Nachweis zu erbringen ist. Diese Dreiteilung („Messpunkt – Schwelle – Evidenz“) wird für alle Prüffälle maschinenlesbar dokumentiert und einer eindeutigen Anforderungs-ID zugeordnet. Messpunkte sind als konkrete, technisch erfassbare Beobachtungen definiert (z. B. Zeitmarken eines ORC-Befehls, Ingest-Sequenzen, Policy-Entscheide), Schwellenwerte geben das akzeptierte Zielband vor (binär oder metrisch), und die Evidenzform spezifiziert das zu archivierende Belegformat (z. B. signierte Protokollauszüge, Artefakt-Digests, AAR-Manifestauszüge). Abnahmen werden run-gebunden erhoben, UTC-synchron gestempelt und so aufbereitet, dass sie sich auf den jeweils gültigen Artefakt- und Release-Stand zurückführen lassen.

Funktionale Abnahmen prüfen, ob das spezifizierte Verhalten eines Dienstes korrekt, idempotent und audittierbar realisiert ist. Der Messpunkt basiert hier typischerweise auf API-Requests/-Responses, Zustandsübergängen und Ereignisfolgen in Orchestrierung und Observability. Die Schwelle ist binär (erfüllt/nicht erfüllt) oder sequenziell (genau eine bestätigte Transition; kein Partial-State), die Evidenz besteht aus signierten Request-Traces, Validator-Berichten und referenzierten AAR-Einträgen. Ein illustratives Beispiel ist das „Szenario-Rollback ohne Nebenschritte“: Die Abnahme gilt als bestanden, wenn erstens eine fehlerhaft präparierte Szenariobeschreibung vom Parser mit Zeilenreferenz zurückgewiesen wird (Messpunkt: Parser-Ergebnis; Schwelle: „invalid“ mit Positionsangabe; Evidenz: signierter Validator-Report), zweitens die Plattform automatisch auf den letzten konsistenten Stand zurückkehrt (Messpunkt: Katalog- und Artefakt-Hashes; Schwelle: Gleichheit mit Referenz; Evidenz: Digests/Signaturen), und drittens die gesamte Abfolge lückenlos protokolliert und signiert ist (Evidenz: AAR-Timeline mit Payload-Hashes).

Nicht-funktionale Abnahmen (Qualitätsattribute) sind metrisch auszuweisen. Für Leistungsziele gelten die in den SLOs definierten Grenzwerte; die Messpunkte folgen der dort festgelegten Methodik (z. B. Ende-zu-Ende-Zeitstempel, P95-Auswertung je Beobachtungsfenster). Eine Anforderung „Time-to-Train für Standard-Range ≤ 30 min“ ist erfüllt, wenn die gemessene Dauer vom freigegebenen Sollzustand bis zu vollständigen Health-Signalen im definierten Beobachtungszeitraum den Zielwert in der vereinbarten Aggregation nicht überschreitet; Evidenz sind die signierten Deploy-Logs und der AAR-Verweis auf die Messreihe. Ähnlich werden Orchestrierungs-Latenzen, Lab-Reset-Zeiten, Query-Antwortzeiten und Ingest-Verlustquoten akzeptanzrelevant belegt; die Berichte sind kohortiert (Run-Typ, Site, Architekturvariante), um Verzerrungen auszuschließen.

Sicherheitsbezogene Abnahmen folgen dem Prinzip fail-closed. Für Lieferkette und Härtung sind binäre Gates maßgeblich: „100 % Signatur-, SBOM- und Schema-Konformität“ bedeutet, dass jeder Import und jede Promotion die entsprechenden Kontrollen bestanden hat; Evidenz sind die Gate-Protokolle (positiver Entscheid, Signatur-/Hash-Listen), Quarantäne-Nachweise bei Verstößen und der WORM-gesicherte Freigabevermerk. Air-Gap-Nachweise gelten als erfüllt, wenn ein definierter Disconnect-Zeitraum ohne externe Abhängigkeiten durchlaufen wurde; Messpunkt sind fehlende Egress-Events bei gleichzeitig vollständiger Funktionsfähigkeit der Plattform, Evidenz sind Telemetrie- und Audit-Logs mit negativer Trefferlage für unerlaubte Ziele. Für das Schlüsselmanagement ist die Abnahme erreicht, wenn Dual-Acceptance, atomare Umschaltung und Widerruf ohne Unterbrechung demonstriert wurden; Evidenz bilden Tresor-Journale, CRL/Trust-Bundle-Stände und Negativtests mit gesperrtem Altmaterial.

Föderationsanforderungen werden über einen Proof-of-Federation abgenommen. Messpunkte sind hier der Handshake (Zertifikatsketten, Agreements, kurzlebige Schlüssel), die Mapping-Konformität (DDS $\leftrightarrow$ HLA-Schema und QoS), die Isolierung (keine Cross-Tenant-Zugriffe, minimale Exportsichten) sowie die Zeitdrift entlang der Kopplungsstrecke. Schwellenwerte sind vollständig vorliegende Handshake-Belege, eine Schema-/QoS-kompatible Abbildung ohne Fehlzuordnungen und eine Drift innerhalb des vereinbarten Toleranzbands; Evidenz sind signierte Handshake-Protokolle, Mapping-Validator-Berichte, Drift-Zeitreihen und Export/Import-Manifeste, jeweils mit AAR-Referenzen.

Die Verfahrensseite der Abnahme ist strikt geregelt. Ergebnisse werden rollenbasiert beurteilt und erfordern für kritische Domänen (Netz, Schlüssel, Lieferkette) eine Vier-Augen-Freigabe. Entscheidungen werden als ADRs mit Verweis auf Anforderungs-ID, Messpunkte, Schwellen, Evidenz und Artefaktstände dokumentiert; AARs referenzieren ihrerseits die verwendeten Paketstände über Versionen und Digests, sodass die Chain-of-Custody geschlossen bleibt. Abweichungen führen automatisiert zu Quarantäne, Rollback oder Entkopplung; die finale Abnahme ist erst zulässig, wenn zugehörige CAPA-Maßnahmen (Corrective/Preventive Actions)

wirksam nachgewiesen wurden. Auf diese Weise wird jede Anforderung nicht nur formal „abgehakt“, sondern prüf- und auditfest in den technischen und organisatorischen Kontext der Plattform eingebettet.

4.11.4 Evidenz, Messdisziplin und Audit

Die Nachweisführung stützt sich auf eine disziplinierte Messpraxis und eine belegfeste Archivierung, die Manipulationsfreiheit, Rückführbarkeit und Vergleichbarkeit über Zeit gewährleisten. Messungen sind run-gebunden instrumentiert; sämtliche Ereignisse tragen UTC-Zeitstempel aus einer lokalen, überwachten Zeitquelle (NTP/GPS/Stratum-Profil). Für die Auswertung sind standardisierte Sichten definiert (kuratierte Query-Presets mit fixierten Filtern, Kardinalitäten und Aggregationsregeln), sodass Berichte unabhängig von Operator:innen, Site oder Architekturvariante konsistent ausfallen. Ausnahmen—namentlich genehmigte Wartungsfenster oder Testläufe außerhalb produktiver Profile—werden explizit markiert und aus den regulären Kennzahlen ausgeschlossen.

Evidenzartefakte sind als erste Bürger des Systems behandelt und folgen einer klaren Taxonomie: (i) Prozessprotokolle (Deploy/Orchestrierung, Admission-Entscheide), (ii) Integritätsnachweise (Signaturen, Hashes, Cosign-Attestationen, SBOM-Fingerprints), (iii) Telemetrie-Extrakte (Metriken, Logs, Traces, Flows) mit Run-Korrelation, (iv) AAR-Manifeste mit Timeline-Referenzen sowie (v) Föderations- und Schlüsselbelege (Handshake-Protokolle, Trust-Bundles, CRL-Stände). Jedes Artefakt besitzt Metadaten zu Erzeuger, Schema-ID, Version, Digest, Signatur, Schutzklasse und Aufbewahrungsfristen. Hochschutzbedürftige Inhalte (z. B. Schlüsselmaterial) werden nicht eingebettet, sondern ausschließlich referenziert (Hash/Signatur/Locator); der Zugriff erfolgt über getrennte, streng kontrollierte Ablagen.

Die Archivierung ist WORM-fähig (Write Once, Read Many) ausgelegt und erzwingt Unveränderlichkeit über Hardware- oder Objektspeicherrichtlinien. Für jede Ablage gelten verbindliche Retention-Pläne und Löschkonzepte im Einklang mit der Datenklassifizierung; Kopien werden georedundant bzw. zonengetrennt gehalten. Die Chain-of-Custody ist geschlossen: Vom Entstehen eines Artefakts über die Validierung bis zur Abnahme existieren lückenlose, signierte Verweise (ADRs ↔ Pipelines/Gates ↔ AAR-Referenzen ↔ Audit-Ablage). Jede Promotion über Quarantäne → Staging → Produktion hinterlässt eine maschinenlesbare Spur.

Zur Sicherung der Messdisziplin werden Messsysteme selbst regelmäßig geprüft. Dazu zählen Kalibrierungen der Zeitbasis (Drift-Checks, Stratum-Wechsel, Monitoring der Offset-Verteilung), Messunsicherheits-Analysen (z. B. Erfassung von Jitter bei Orchestrierungs-Bestätigungen) sowie Reproduzierbarkeits-Tests (Wiederholungsläufe mit identischen Seeds, konstanten Startbedingungen und kontrollierten Hintergrundlasten). Randomisierte Workloads (z. B. Traffic-Generatoren) verpflichten zur Seed-Dokumentation, damit Auswertungen deterministisch wiederholbar sind. Die Versionen aller Query-Sichten und Dashboards sind fixiert und werden bei Änderungen semantisch versioniert.

Audits sind als systematische Wirksamkeitsprüfung konzipiert und erfolgen in einem festgelegten Takt (intern) sowie anlassbezogen (extern). Bewertet werden: (i) Durchsetzung (Policy-Trefferquoten, Block-/Quarantäne-Raten, Validierungslatenzen in Gates), (ii) Stabilität (SLO-Konformität über Zeit und Kohorten, Fehlerbudgetverbräuche), (iii) Prozessreife (Vollständigkeit von ADRs/AARs, Termintreue bei Freigaben, Nachweisdrill-Ergebnisse). Die Stichprobenziehung ist risikobasiert (höhere Dichte bei kritischen Zonen, Lieferkette, Föderation, HIL). Auditfestigkeit setzt Unabhängigkeit der Prüfinstanz, dokumentierte Prüfpfade und die Reproduzierbarkeit von Befunden aus Rohbelegen voraus.

Abweichungen werden technisch fail-closed behandelt und organisatorisch über CAPA-Prozesse (Corrective and Preventive Actions) geschlossen. Jeder Befund enthält eine präzise Fundstelle

(Regel/Schema/Version), Kontext (Run-ID, Site, Artefakt-Digest), eine Ursachenanalyse entlang der Kategorien Konfiguration, Kapazität, Implementierung, Datenqualität sowie terminierte Korrektur- und Präventionsmaßnahmen. Die Wirksamkeit wird in Folgeläufen nachgewiesen; erst dann gilt der CAPA-Eintrag als geschlossen. Kritische Befunde können temporäre Gating-Maßnahmen (Rollback, Quarantäne, Entkopplung föderierter Strecken) auslösen.

Zur Wahrung von Datensparsamkeit und Schutzbedarf sind minimale Evidenzpakete für Standard-, Sicherheits- und Föderationsprüfungen definiert. Diese Pakete reichen für die Verifikation der Kriterien aus, ohne unnötige Detailoffenlegung. Wo Forschungs- oder Lehrzwecke eine Weitergabe erfordern, kommen Anonymisierungspfade (Pseudonyme, Hash-Maskierung, Reduktion von Kardinalitäten) zum Einsatz; die Ableitungsregeln werden dokumentiert und versioniert, um analytische Konsistenz zu sichern.

Schließlich gewährleistet ein Evidenz-Lebenszyklus die Anschlussfähigkeit an Abnahme und Governance: Prüfplanung → Messung/Erhebung → Validierung/Signatur → WORM-Archiv → Audit → Lessons Learned. Die daraus resultierenden Trendberichte (z. B. Entwicklung der Query-SLOs, Drift in Föderationsstrecken, Häufigkeit von Policy-Verstößen) dienen als unmittelbarer Input für Kapazitätsplanung, Runbooks und Policy-Weiterentwicklung. Auf diese Weise wird Evidenz nicht nur gesammelt, sondern systematisch in Steuerungsentscheidungen überführt—nachvollziehbar, reproduzierbar und auditfest.

4.11.5 PoC/MVP-Fahrplan (Iterationen und Meilensteine)

Der Fahrplan strukturiert die Einführung der Trainingsplattform als Folge kontrollierter Experimente. Jede Iteration reduziert eine klar benannte Unsicherheit, erzeugt prüfbare Evidenz und hinterlässt eine audittierbare Spur (signierte Zwischen-AARs und ADRs). Die Stufen sind so geschnitten, dass sie unter Air-Gap-Bedingungen durchführbar sind, keine unnötigen Vorabinvestitionen erzwingen und bei Regressionen einen geordneten Rücksprung ermöglichen. Entry-/Exit-Kriterien sind objektiv messbar; Abhängigkeiten, Annahmen und Risiken werden pro Iteration offengelegt.

Iteration 0 – Basisbereitstellung. Ziel ist ein minimaler, funktionsfähiger Validierungsraum. Eingeschlossen sind Zeitquelle (lokal, überwacht), PKI/IdP (offline-fähig), Registry/Git-Mirrors sowie eine schlanke Observability-Grundlage. Der Schwerpunkt liegt auf Messdisziplin (UTC-Synchronität, run-gebundene Korrelation) und auf der Lieferkette: Importpfade sind ausschließlich über Quarantäne möglich, Signatur-/SBOM-Prüfungen blockieren nicht konforme Artefakte. Exit ist erreicht, wenn Disconnect-Smoke-Tests ohne externe Abhängigkeiten bestehen und die Gates fail-closed reagieren (nachweislich blockierte, unsignierte Testpakete).

Iteration 1 – IaC-Durchstich. Diese Stufe etabliert die vollständige Plan/Apply/Destroy-Kette bis Staging. Terraform/Ansible (Architektur A) bzw. GitOps/Helm/Kustomize (Architektur B) liefern deterministische Pläne und reproduzierbare Deployments. Zulieferungen passieren weiterhin Quarantäne → Staging → Produktion im Air-Gap. Exit setzt idempotente Applies, deterministische Rebuilds (mehrfach identische Hashes) und nachvollziehbare Drift-Detektion voraus; die Evidenz umfasst signierte Pipeline-Protokolle, Artefakt-Digests und ein Kurz-AAR des Durchstichs.

Iteration 2 – Szenario-Lebenszyklus & Hands-on. Im Fokus stehen deklarative Szenariobeschreibungen (Parser-Gates, Vier-Augen-Freigabe), Katalog-Prozesse und Hands-on-Funktionen (Reset/Replay, Scoring). Die Iteration prüft, ob aus Szenario-Code konsistent lauffähige Trainingsumgebungen entstehen, ob Fehlmodelle mit Fundstelle abgewiesen werden und ob Labs zustandsrein zurückgesetzt werden. Exit ist erreicht, wenn Time-to-Train und Reset-Zielwerte im Referenzlauf eingehalten und die Ereignisse end-to-end korreliert sind (AAR-Timeline mit Payload-Hashes).



Iteration 3 – Observability & AAR. Diese Stufe verankert run-gebundene Ingest-Pfade (OTLP, Syslog, NetFlow/IPFIX) und standardisierte Sichten für Analyse und Triage. Zusätzlich wird die AAR-Erzeugung mit signierten Manifesten und deterministischen Replays aufgebaut. Exit umfasst eingehaltene Query-SLOs für die definierten Dashboards und mindestens ein vollständiges AAR mit gültiger Signatur, SBOM-Fingerprints und referenzierten Artefakten (keine Einbettung hochschutzbedürftiger Inhalte).

Iteration 4 – Föderations-Pilot. Ziel ist eine kontrollierte Inter-Site-Kopplung: HLA/DIS (Architektur A) bzw. DDS↔HLA-Bridge (Architektur B) werden mit kurzlebigen Schlüsseln und dedizierten Föderations-Strecken betrieben. Validiert werden Trust Establishment, Schema/QoS-Konformität und Timeline-Drift innerhalb des vereinbarten Korridors; Exportsichten bleiben minimal und policy-konform. Exit liefert einen signierten Proof-of-Federation (Handshake-Protokolle, Mapping-Reports, Drift-Zeitreihen) sowie klare Entkopplungsmechanismen für den Fehlerfall.

Iteration 5 – HIL-Adapter. Hier wird die Real-Integration unter Guards nachgewiesen: Registrierung, Policy- und Rate-Limit-Durchsetzung, Positiv-/Negativtests (z. B. Abweisen nicht genehmigter Protokolle). Ereignisse aus Realquellen sind eindeutig markiert, und kein Verkehr überschreitet die definierten Barrieren. Exit ist erreicht, wenn die Guard-Kontrollen ohne Ausnahme greifen, die Markierung in Observability und AAR konsistent erscheint und ein Emulations-Fallback technisch belegt ist.

Iteration 6 – Last & Skalierung. Schwerpunkt sind Parallelbetrieb gemäß Kapazitätsplanung und die Verteidigung gegen Noisy-Neighbor-Effekte. Stufen-, Burst- und Soak-Profilen belasten die dimensionierenden Achsen (CPU, RAM, IOPS, Netz). Admission-Gates wirken als harte Grenze; kritische Dienste werden auf Stabilität (keine Evictions/Throttling, konstante Latenzen) überwacht. Exit ist erreicht, wenn die SLO-Zielwerte unter Last eingehalten sind und die zulässige Parallelität empirisch bestätigt oder angepasst wurde; Evidenz sind Laufzeitprofile und SLO-Berichte je Kohorte (Run-Typ, Site, Architekturvariante).

Iteration 7 – Betriebsreife. Die Abschlusstufe prüft Wiederherstellung (Backup/Restore, DR-Drills), Schlüsselrotation mit Dual-Acceptance/Widerruf und Patch-Fenster mit stufenweisem Rollout und Rollback-Garantie. Exit verlangt das Erreichen der RTO/RPO-Ziele, bestandene Rotations-Nachweise (Tresor-Journal, CRLs/Trust-Bundles, Negativtests) und den Abschluss aller CAPA-Restpunkte. Das Ergebnis ist ein belastbarer Betriebsnachweis mit vollständiger Evidenzkette.

Durchführungsprinzipien über alle Iterationen.

- Risikobasierte Priorisierung: Lieferkette, Air-Gap, Föderation und Schlüsselmanagement erhalten Vorrang; Leistungs- und Skalierungsfragen folgen eng getaktet.
- Gating & Rücksprung: Nichtkonformität führt automatisch zu Quarantäne/Rollback/Entkopplung; ein Rollback-Plan ist Teil jedes Entry-Katalogs.
- Rollen & Freigaben: Kritische Schritte (Netz-Änderungen, Artefakt-Promotion, Schlüsselrotation) erfordern Vier-Augen-Freigaben; Zuständigkeiten (Plattform-Ops, Security/Governance, Übungsleitung) sind schriftlich fixiert.
- Evidenz als Produkt: Jede Stufe erzeugt signierte Zwischen-AARs und ADRs mit Annahmen, Entscheidungen, Abnahmen und offenen Punkten; hochschutzbedürftige Belege werden referenziert und WORM-gesichert.
- Architekturübergreifende Vergleichbarkeit: Prüflogik und Messmethodik sind in A und B identisch; Unterschiede bestehen nur in der Durchsetzung (z. B. Admission-Gates vs. Gateway-ACLs). So bleiben Resultate transferierbar und der Variantenvergleich belastbar.



Mit dieser Sequenz entsteht ein nachvollziehbarer Pfad von der minimalen Referenz zur produktionsnahen Validierung. Jede Iteration erhöht die Beweisdichte, reduziert Restunsicherheit und belegt die Einsatzreife der Plattform in beiden Referenzarchitekturen anhand objektiver, reproduzierbarer Kriterien.

4.12 Roadmap & Risiken

Dieses Kapitel übersetzt den Architekturentwurf sowie den in Kapitel 4.11.5 beschriebenen PoC-/MVP-Fahrplan in eine umsetzungsorientierte Roadmap und ein konsolidiertes Risiko-Register. Im Mittelpunkt steht damit nicht mehr die Frage, wie eine geeignete Zielarchitektur für die Trainingsplattform aussieht, sondern wie diese Zielarchitektur unter realen organisatorischen, zeitlichen und betrieblichen Randbedingungen schrittweise eingeführt und verstetigt werden kann. Die Roadmap fungiert dabei als Bindeglied zwischen den konzeptionellen Ergebnissen der vorangegangenen Kapitel und der praktischen Implementierung in Form von Projekten, Iterationen und Betriebsprozessen.

Ausgehend vom in Kapitel 4.2 definierten Zielbild sowie den in Kapitel 4.5 und 4.6 beschriebenen Referenzarchitekturen werden zwei komplementäre Zeithorizonte betrachtet: ein kompakter Pfad mit etwa sechs Monaten bis zur Bereitstellung einer einsatzfähigen Minimalversion der Plattform (MVP) und ein erweiterter Pfad mit ungefähr zwölf Monaten bis zur Annäherung an das angestrebte Zielbild. Beide Pfade sind grundsätzlich sowohl für die Referenzarchitektur A (VM-zentriert) als auch für die Referenzarchitektur B (cloud-native) anwendbar. Architekturspezifische Schwerpunkte, Unterschiede in der organisatorischen und betrieblichen Komplexität sowie Implikationen für den Einführungsweg werden in den nachfolgenden Unterkapiteln jeweils explizit herausgearbeitet, ohne die grundsätzliche Vergleichbarkeit der Pfade zu verlieren. Parallel zur zeitlichen Planung adressiert dieses Kapitel die Risikoperspektive der Einführung. Das konsolidierte Risiko-Register ergänzt die in den Kapiteln 5.6 und 6.6 aufgeführten architekturspezifischen Risikokataloge um eine programm- und transformationsbezogene Sichtweise. Im Fokus stehen dabei Risiken, die sich aus der schrittweisen Einführung, der Migration bestehender Übungslandschaften, der Etablierung neuer Betriebs- und Governance-Modelle sowie aus der langfristigen Verstetigung der Plattform ergeben. Zu jedem Risiko werden auf einem abstrahierten Niveau mögliche Gegenmaßnahmen und Steuerungsansätze beschrieben, die in den folgenden Unterkapiteln systematisch mit den in der Roadmap definierten Phasen und Meilensteinen verknüpft werden. Die nachfolgenden Unterkapitel spezifizieren diese Elemente im Detail: Zunächst werden die grundlegenden Annahmen und Rahmenbedingungen der Planung erläutert, anschließend werden die Roadmaps für den sechs- und zwölfmonatigen Horizont ausgeführt und um einen Einführungs- und Migrationsplan ergänzt. Abschließend wird das Risiko-Register vorgestellt, das die identifizierten Transformationsrisiken bündelt und den Brückenschlag zwischen Architektur, Roadmap und operativem Betrieb herstellt.

4.12.1 Zielbild und Annahmen

Ausgangspunkt der Roadmap ist ein klar umrissenes Zielbild der Trainingsplattform sowie eine Reihe expliziter Annahmen zu technischen, architektonischen und organisatorischen Rahmenbedingungen. Diese dienen als Referenzrahmen für die in den nachfolgenden Unterkapiteln beschriebenen Ausbaustufen und Risikobetrachtungen und stellen sicher, dass die Roadmap nachvollziehbar auf die in den Kapiteln 4.2, 4.5, 4.6 und 4.11 hergeleiteten Anforderungen und Architekturentscheidungen rückführbar bleibt.

Technisches Zielbild

Technisch zielt die Roadmap auf eine air-gap-fähige Trainingsplattform ab, die die in Kapitel 4.3 spezifizierten Trainingsformate – insbesondere Cyber-Range-Szenarien, Hands-on-Labs, föderierte Übungen mit Partnerorganisationen sowie Hardware-in-the-Loop-(HIL-)Integration – in konsistenter Weise unterstützt. Die Plattform soll diese Formate nicht nur funktional „ermöglichen“, sondern qualitativ so bereitstellen, dass die definierten nicht-funktionalen Anforderungen erfüllt werden. Dazu zählen insbesondere Vorgaben zu Provisionierungszeiten (z. B. Wiederherstellung definierter Ausgangszustände vor Übungsbeginn), Orchestrierungs-Latenzen (z. B.

Reaktionszeiten der Plattform auf Steuerbefehle), Reset-Zeiten (z. B. Zurücksetzen von Runs zwischen Übungsdurchgängen) sowie serviceorientierte Zielgrößen (Service Level Objectives, SLOs) für Verfügbarkeit und Performance. Ein zentrales Merkmal des Zielbilds ist die Fähigkeit zum Betrieb in unterschiedlich stark abgeschotteten Umgebungen bis hin zu weitgehend vom Internet entkoppelten Setups („Air-Gap“). Die Plattform muss daher in der Lage sein, alle für den Trainingsbetrieb erforderlichen Artefakte (Images, Container-Images, Pakete, Konfigurationen, Policies) über geprüfte, kontrollierte Importwege zu beziehen und in einer lokalen Infrastruktur vorzuhalten. Die in den nachfolgenden Unterkapiteln beschriebenen Roadmap-Phasen adressieren schrittweise die Herstellung dieser Eigenschaften – zunächst für einen lokal begrenzten, MVP-artigen Scope, anschließend für ein erweitertes, föderations- und HIL-fähiges Zielbild.

Architekturvarianten

Das Zielbild ist so formuliert, dass es prinzipiell von beiden in den Kapiteln 4.5 und 4.6 beschriebenen Referenzarchitekturen realisiert werden kann: der VM-zentrierten Referenzarchitektur A und der cloud-nativen Referenzarchitektur B auf Basis von Kubernetes, Service-Mesh und DDS/HLA-Bridge. Die Roadmap selbst wird bewusst variantenneutral formuliert, d. h. sie beschreibt Phasen, Aktivitäten und Meilensteine in einer Form, die sowohl für eine VM-zentrierte als auch für eine containerisierte Ausprägung gültig ist. Gleichzeitig ist davon auszugehen, dass sich die architekturenspezifische Ausprägung einzelner Roadmap-Schritte deutlich unterscheidet – etwa im Hinblick auf den Aufbau der Infrastruktur, die Ausgestaltung von Automatisierung und Observability oder die Einführung von Governance-Mechanismen (IaC vs. GitOps, Hypervisor-Cluster vs. Kubernetes-Cluster, HLA-Föderation vs. DDS-Domänen mit HLA-Bridge). Wo solche Unterschiede relevant sind, werden sie in den jeweiligen Unterkapiteln als Architektur-Delta kenntlich gemacht. Auf diese Weise bleibt die Roadmap konsistent vergleichbar, ohne die Besonderheiten von Referenzarchitektur A und B zu nivellieren.

Organisatorischer Rahmen

Organisatorisch geht die Roadmap davon aus, dass die Trainingsplattform nicht in einem einzigen Schritt, sondern in mehreren Ausbaustufen eingeführt wird. In einem ersten Schritt wird eine Minimalversion (MVP) mit begrenztem Szenariokatalog, einem klar umrissenen Satz von Trainingsformaten und einem primär Single-Site-Betrieb etabliert. In dieser Phase steht die Etablierung stabiler Betriebs- und Governance-Prozesse im Vordergrund, etwa in Form von Architekturentscheidungsdocumenten (Architectural Decision Records, ADRs), Runbooks für wiederkehrende Betriebsabläufe und Policies-as-Code zur technischen Durchsetzung definierter Sicherheits- und Governance-Regeln. Aufbauend auf diesem MVP wird in weiteren Iterationen ein schrittweiser Ausbau in Richtung Multi-Site-Föderation (z. B. Einbindung weiterer Übungsstandorte oder Partner) und HIL-Einsatz vorgesehen. Dies umfasst unter anderem die Ausweitung des Szenariokatalogs, die Einführung und Härtung föderierter Verbindungen sowie die Integration physischer Komponenten über standardisierte Adapter und Schutzmechanismen. Die nachfolgenden Unterkapitel zur Roadmap konkretisieren diese Entwicklungslinien in Form von Phasenmodellen und exemplarischen Meilensteinen.

Zeitliche Orientierung und Anpassungsbedarf

Die in diesem Kapitel verwendeten Zeithorizonte von rund sechs Monaten bis zu einer einsatzfähigen MVP-Plattform und etwa zwölf Monaten bis zum erweiterten Zielbild sind ausdrücklich als Orientierungswerte zu verstehen. Sie reflektieren typische Erfahrungswerte für Vorhaben vergleichbarer Komplexität unter der Annahme einer hinreichenden Ressourcenausstattung und klarer Entscheidungswege. Konkrete Planstände, verfügbare Budgets und Personalkapazitäten, die Dauer von Beschaffungs- und Genehmigungsprozessen sowie

organisationsspezifische Rahmenbedingungen (z. B. sicherheitsbehördliche Freigaben) können diese Zeithorizonte erheblich beeinflussen.

Entsprechend ist die Roadmap so gestaltet, dass sie als strukturierender Rahmen genutzt und an projektspezifische Gegebenheiten angepasst werden kann. Die nachfolgenden Unterkapitel machen explizit, an welchen Stellen Verdichtungen oder Dehnungen der Phasen möglich sind, wie Abhängigkeiten zwischen Aktivitäten zu berücksichtigen sind und welche Risiken sich aus Abweichungen vom skizzierten Pfad ergeben können.

4.12.2 Sechs Monate Roadmap zum MVP

Der kompakte 6-Monats-Pfad beschreibt die schrittweise Entwicklung zu einem betriebsnahen Minimal Viable Product (MVP) der Trainingsplattform. Im Fokus steht eine erste, produktionsnahe Ausprägung, die bereits wesentliche Anforderungen an Cyber-Range-Szenarien, Hands-on-Labs, Observability und After-Action-Reporting (AAR) erfüllt, ohne jedoch das volle Zielbild – insbesondere hinsichtlich umfassender Föderation und HIL-Integration – bereits vollständig auszuschöpfen. Föderationsfunktionen und HIL-Anbindung werden in diesem Pfad primär als vorbereitete, architektonisch mitgedachte, aber noch nicht in der Breite ausgerollte Optionen adressiert. Die nachfolgenden Phasen strukturieren den 6-Monats-Pfad in klar abgegrenzte Zeitabschnitte mit jeweils definierten Schwerpunkten, Abhängigkeiten und Ergebnissen. Sie sind grundsätzlich sowohl auf die VM-zentrierte Referenzarchitektur A als auch auf die cloud-native Referenzarchitektur B anwendbar; spezifische Ausprägungen werden jeweils als architekturenspezifische Schwerpunkte kenntlich gemacht.

4.12.2.1 Phase 1 (Monat 0–2): Foundations & Basisbereitstellung

In der ersten Phase werden die technischen und organisatorischen Grundlagen geschaffen, auf denen alle weiteren Ausbaustufen aufsetzen. Ziel ist die Etablierung eines minimalen, aber konsistenten Validierungsraums, der deterministische Bereitstellung, reproduzierbare Konfiguration und grundlegende Offline-Tauglichkeit sicherstellt.

Schwerpunkte:

- Aufbau der Basisinfrastruktur gemäß gewählter Referenzarchitektur
 - Architektur A: Aufbau eines gehärteten Hypervisor-Clusters einschließlich VM-Management, grundlegender Speicher- und Netzkonfiguration sowie einer Netzsegmentierung, die das in der Sicherheitsarchitektur definierte Zonenmodell abbildet. Parallel dazu Einrichtung initialer HLA/DIS-Strecken zur Kopplung erster Simulatoren und Übungsumgebungen.
 - Architektur B: Aufbau eines oder mehrerer Kubernetes-Cluster als Plattformbasis, Einrichtung einer lokalen Container-Registry und von Git-Mirrors, Grundkonfiguration eines Service-Mesh (mTLS-fähige Control-Plane, initiale Sidecar-Konfiguration) sowie Definition erster DDS-Domänen und einer Basis-DDS/HLA-Bridge für spätere Föderationsszenarien.
- Etablierung grundlegender Vertrauensanker und Artefaktversorgung
 - Aufbau einer vertrauenswürdigen Zeitquelle (z. B. lokal synchronisierte NTP-Server mit ggf. vorgelagerter GPS-Referenz), einer internen PKI/IdP-Grundlage sowie lokaler Artefakt-Mirrors. Letztere müssen in der Lage sein, Images, Pakete und Konfigurationen inkl. Signatur- und SBOM-Informationen aufzunehmen und zu prüfen. Hierdurch wird die Basis für eine nachvollziehbare und auditierbare Lieferkette sowie für den späteren Air-Gap-Betrieb gelegt.

- Umsetzung erster IaC-/GitOps-Pipelines und Observability-Grundlage
 - Einführung eines initialen Satzes von IaC- bzw. GitOps-Pipelines, die typische Operationen wie „Plan“, „Apply“ und „Destroy“ für die Basisinfrastruktur abdecken. Diese werden zunächst auf eine Staging-Umgebung ausgerichtet, um Änderungen risikoreduziert erproben zu können. Ergänzend wird eine minimale Observability-Infrastruktur bereitgestellt (Metriken und Logs aus Kernkomponenten, zentrale Run-ID-Führung), um den Zustand der Plattform kontinuierlich erfassen und bewerten zu können.
- Validierung von Offline- und Importpfaden
 - Bereits in dieser frühen Phase werden erste Disconnect-Tests durchgeführt, um die Robustheit der Plattform bei Ausfall externer Verbindungen zu überprüfen. Importpfade für Artefakte werden ausschließlich über definierte, geprüfte Quarantäne-Strecken betrieben, sodass die Einhaltung von Sicherheits- und Lieferkettenanforderungen von Beginn an eingeübt wird.

Ergebnis: Das Ergebnis der Phase 1 ist ein minimaler, funktionsfähiger Validierungsraum, in dem Infrastruktur und zentrale Plattformkomponenten deterministisch und reproduzierbar bereitgestellt werden können. Die wesentlichen Vertrauensanker (Zeitquelle, PKI, Artefakt-Mirrors) sind etabliert, und die Offline-Tauglichkeit der Grundkonfiguration ist nachweislich getestet. Dieser Zustand bildet die Grundlage für den in Phase 2 folgenden Aufbau des eigentlichen Plattformkerns und erster Referenzszenarien.

4.12.2.2 Phase 2 (Monat 2–4): MVP-Plattformkern & Referenzszenarien

In Phase 2 verschiebt sich der Schwerpunkt von der reinen Basisbereitstellung der Infrastruktur hin zum Aufbau eines betriebsnahen Plattformkerns, der bereits konkrete Trainingsformate unterstützt. Ziel dieser Phase ist es, einen ersten, konsistenten Ausschnitt der Zielform zu realisieren, auf dem exemplarische Szenarien abgebildet, gesteuert und ausgewertet werden können, ohne den Umfang eines vollständigen Zielbilds vorwegzunehmen.

Schwerpunkte

- Umsetzung eines initialen Szenariokatalogs
 - Im Mittelpunkt steht die Implementierung eines ersten, kuratierten Szenariokatalogs. Dieser umfasst mindestens ein komplexes Cyber-Range-Referenzszenario mit mehrschichtigen Übungsnetzen, unterschiedlichen Rollenbildern und realitätsnahen Angriffs- und Verteidigungsoptionen sowie ein bis zwei Hands-on- beziehungsweise HTB-artige Labs. Diese Labs zeichnen sich durch die Möglichkeit aus, Szenarien automatisiert auf definierte Ausgangszustände zurückzusetzen, Durchläufe zu wiederholen (Replay) und individuelle wie auch teambezogene Leistungen über Scoring-Mechanismen auswertbar zu machen. Die ausgewählten Szenarien fungieren als „Leuchtturmfälle“, an denen Funktionsumfang, Usability und Auswertbarkeit des MVP bewertet und weiterentwickelt werden können.
- Fertigstellung der Orchestrierungs-Funktionen
 - Parallel dazu werden die zentralen Orchestrierungs-Funktionen der Plattform ausgebaut und in einen betriebsnahen Zustand überführt. Dazu gehören insbesondere Start-, Pause- und Reset-Funktionen für Szenarien, die gezielte Einbringung von Ereignissen (Event-Injection, etwa zur Simulation von



Störungen oder Eskalationen) sowie ein Runden- und Teilnehmermanagement, das die Zuordnung von Nutzenden zu Runs, Rollen und Ressourcen unterstützt. Diese Funktionen werden durch eine einfache, klar definierte Governance für ad-hoc-Ereignisse ergänzt, sodass spontane Anpassungen während laufender Übungen möglich sind, ohne die Nachvollziehbarkeit von Abläufen und AAR-Ergebnissen zu gefährden.

- Ausbau der Observability zur run-gebundenen Telemetrie (MELT)
 - Die in Phase 1 etablierte Observability-Grundlage wird in dieser Phase zu einer run-gebundenen Telemetrie-Infrastruktur weiterentwickelt. Ziel ist eine konsolidierte Erfassung von Metriken, Events, Logs und Traces (MELT) auf Ebene einzelner Trainingsläufe. Auf dieser Basis werden Dashboards aufgebaut, die zentrale Kennzahlen wie Provisionierungszeiten, Orchestrierungs-Latenzen, Reset-Zeiten und Ressourcenauslastung sichtbar machen. Zudem werden die technischen Voraussetzungen geschaffen, um aus diesen Daten strukturierte AAR-Artefakte zu generieren, die sowohl operative Lessons Learned als auch formale Nachweisführung unterstützen.
- Abdeckung grundlegender Sicherheits- und Segmentierungsanforderungen
 - Um einen sicheren MVP-Betrieb zu ermöglichen, werden in Phase 2 die grundlegenden Sicherheits- und Segmentierungsanforderungen in der Plattform verankert. Dazu gehören die Einführung von Zero-Trust-Segmenten auf Infrastruktur- bzw. Workload-Ebene, ein rollenbasiertes Berechtigungsmodell (RBAC) für administrative und didaktische Rollen, die Umsetzung von Deny-by-Default-Policies in relevanten Komponenten sowie ein konsistentes Audit-Logging sicherheitsrelevanter Aktionen. Diese Maßnahmen bilden die Grundlage für weitergehende Härtings- und Compliance-Aktivitäten in späteren Phasen.

Architektur-spezifische Schwerpunkte

- Referenzarchitektur A (VM-zentriert)
 - In der VM-zentrierten Ausprägung liegt der Fokus auf der konsequenten Nutzung von Golden Images für wiederkehrende Rollen (z. B. Simulationsknoten, Orchestrierungs- und Auswertungs-VMs), dem systematischen Einsatz von VM-Snapshots und Clones zur schnellen und deterministischen Bereitstellung von Szenarien sowie der Härtung der Netz- und Systemkonfiguration auf Hypervisor- und Firewall-Ebene. Hinzu kommt die Konfiguration und Erprobung von HLA-Föderationsgateways, um erste, klar abgegrenzte Kopplungsszenarien mit externen Simulatoren oder Übungsumgebungen zu unterstützen, ohne bereits eine umfassende Föderationslandschaft zu etablieren.
- Referenzarchitektur B (cloud-native)
 - In der cloud-nativen Variante stehen die Etablierung stabiler GitOps-Synchronisationspfade, einschließlich Signatur-, Review- und Promotionsprozessen, sowie die Einführung und Härtung von Admission-Policies (z. B. OPA-/Gatekeeper-/Kyverno-ähnliche Mechanismen) im Vordergrund. Ergänzend werden Service-Mesh-Policies mit mTLS-Absicherung als Standard („mTLS by default“) implementiert und Namespaces sowie NetworkPolicies als zentrale Mittel zur Mandanten- und Zonen-Trennung

eingesetzt. Diese Bausteine stellen sicher, dass der MVP-Plattformkern bereits unter einem Zero-Trust-Paradigma operiert und späteren Skalierungs- und Föderationsanforderungen gewachsen ist.

Ergebnis: Mit Abschluss der Phase 2 liegt ein betriebsnaher MVP-Plattformkern vor, auf dem ein klar definierter Satz von Trainingsformaten – exemplarisch ein komplexes Cyber-Range-Szenario und erste Hands-on-Labs – reproduzierbar, steuerbar und anhand geeigneter Kennzahlen messbar betrieben werden kann. Die Plattform verfügt über grundlegende Orchestrierungs-, Observability- und Sicherheitsmechanismen, die einen realen, wenn auch zunächst noch in Umfang und Vielfalt begrenzten Trainingsbetrieb ermöglichen und gleichzeitig als belastbare Basis für Härtung, Skalierung und funktionale Erweiterungen in den folgenden Roadmap-Phasen dienen.

4.12.2.3 Phase 3 (Monat 4–6): Härtung, Testkampagnen & lokale Einsatzreife

In Phase 3 liegt der Schwerpunkt auf der Härtung, systematischen Validierung und betriebsorganisatorischen Konsolidierung der in den vorangegangenen Phasen aufgebauten MVP-Plattform. Ziel ist es, den Status von einer technisch funktionalen, aber noch experimentell geprägten Umgebung zu einer lokal einsatzreifen Trainingsplattform zu heben, die unter definierten Rahmenbedingungen regulär betrieben werden kann. Dabei werden die in den Kapiteln 4.5, 4.6, 4.8.3 und 4.11 beschriebenen Anforderungen und Leitlinien in konkret überprüfbare Test- und Betriebsartefakte überführt.

Schwerpunkte

- Durchführung strukturierter Testkampagnen
 - Zentrale Aktivität dieser Phase ist die Durchführung der in Kapitel 4.11 beschriebenen Testkampagnen mit explizitem Fokus auf den MVP-Scope. Dies umfasst Funktions- und Integrationstests der wesentlichen Plattformdienste (z. B. Orchestrierung, Szenariobereitstellung, Observability), Last- und Performancetests unter realitätsnahen Nutzungsszenarien (z. B. parallele Runs, unterschiedliche Rollenverteilung) sowie Sicherheits- und – soweit im MVP-Scope vorgesehen – erste Föderationstests. Die Testkampagnen dienen dazu, die Einhaltung der definierten Qualitätsziele und Service Level Objectives (SLOs) nachzuweisen, systematisch Schwachstellen zu identifizieren und eine belastbare Evidenzbasis für Abnahmeentscheidungen und spätere Audits zu schaffen.
- Etablierung eines belastbaren Betriebsmodells
 - Parallel zur Testdurchführung wird ein Betriebsmodell ausgearbeitet und eingeführt, das die wesentlichen Day-2-Operations abdeckt. Hierzu gehören insbesondere Runbooks für Provisionierung und Deprovisionierung von Szenarien und Ressourcen, Routinen für den regulären Betrieb (Monitoring, Kapazitätsplanung, Störungsbearbeitung), definierte Prozesse für Backup und Restore von kritischen Daten und Konfigurationen, Verfahren für den Import von Artefakten über Quarantäne- und Freigabestufen sowie die Festlegung von Patch-Fenstern und Verfahren zur Schlüsselrotation. Das Betriebsmodell soll sowohl sicherstellen, dass der MVP-Betrieb im lokalen Kontext zuverlässig funktioniert, als auch als Blaupause für spätere Skalierung (z. B. weitere Standorte, erweiterter Szenariokatalog) dienen.
- Härtung der Plattform entlang definierter Leitlinien



- Aufbauend auf den architekturspezifischen Sicherheits- und Härtingsmaßnahmen aus Kapiteln 4.5 und 4.6 sowie dem übergreifenden Sicherheits- und Compliance-Rahmen aus Kapitel 9 wird die Plattform in dieser Phase gezielt gehärtet. Dies umfasst unter anderem:
 - Vertiefte Netz-Härtung (Segmentierung, Filterregeln, Protokollierung, Zero-Trust-Umsetzung),
 - Sicherung und Überwachung der Lieferkette (Signatur- und SBOM-Prüfungen, Quarantäne- und Promotionsprozesse für Artefakte),
 - Ausbau und Absicherung von Tresor- und Schlüsselverwaltungsmechanismen (z. B. Umgang mit Root- und Intermediate-Keys, Rollentrennungen),
 - konsequente Umsetzung von Policies-as-Code und deren Integration in CI-/GitOps- bzw. IaC-Pipelines,
 - Weiterentwicklung der Observability- und Audit-Sichten hin zu einer konsistenten, prüfbaren Sicht auf Betriebszustände, Sicherheitsereignisse und Architekturkonformität.
- Ziel ist eine Plattform, die nicht nur funktional den Anforderungen genügt, sondern auch unter Sicherheits- und Compliance-Gesichtspunkten belastbar ist.
- Vorbereitung von Föderations- und HIL-Anbindung
 - Auch wenn föderierte Übungen und HIL-Anbindung im 6-Monats-Pfad noch nicht flächendeckend ausgerollt werden, werden in dieser Phase die entsprechenden Grundlagen gelegt. Typischerweise geschieht dies in Form von Pilot-Strecken mit klar begrenztem Scope, etwa durch den Aufbau einzelner Föderationslinks zu ausgewählten Partnern oder den testweisen Anschluss spezifischer HIL-Komponenten. Diese Pilotierungen dienen dazu, technische und organisatorische Fragestellungen (z. B. Namensraum- und Zonenabgrenzung, Guard-Mechanismen, Abnahmeverfahren) frühzeitig zu klären und zu dokumentieren, ohne den MVP-Betrieb mit umfassenden Kopplungsszenarien zu überfrachten. Die dabei gewonnenen Erfahrungen fließen in die spätere Ausgestaltung des erweiterten 12-Monats-Pfads ein.

Ergebnis: Mit Abschluss der Phase 3 erreicht die Plattform den Status der lokalen Einsatzreife für den Trainingsbetrieb an einem Standort. Die in den vorhergehenden Phasen geschaffenen Funktionen und Strukturen sind durch systematische Testkampagnen validiert, die wesentlichen SLOs sind definiert und durch Messdaten hinterlegt, und zentrale Betriebsprozesse sind dokumentiert, eingeübt und organisatorisch verankert.

Darüber hinaus liegt eine dokumentierte Evidenzkette vor, die die Nachvollziehbarkeit von Architekturentscheidungen, Konfigurationen, Testergebnissen und Betriebszuständen unterstützt und damit sowohl für interne Governance-Zwecke als auch für externe Prüfungen (z. B. sicherheitsbehördliche Audits) nutzbar ist. Auf dieser Basis können weitere Ausbaustufen – insbesondere der Übergang zu Multi-Site-Föderation, erweiterter HIL-Integration und einer breiteren Skalierung des Szenariokatalogs – geplant und im Rahmen des erweiterten Roadmap-Pfads umgesetzt werden.

4.12.3 Roadmap – erweiterter Pfad (~12 Monate bis Zielbild)

Der erweiterte 12-Monats-Pfad baut auf der in den vorherigen Abschnitten beschriebenen MVP-Plattform auf und adressiert den Übergang von einer lokal einsatzfähigen Minimalversion hin zu

einer weitgehend ausgebauten Zielarchitektur. Während der kompakte 6-Monats-Pfad auf die Herstellung der Grundfunktionalität, der lokalen Betriebssicherheit und der Nachweisfähigkeit des Systems ausgerichtet ist, fokussiert der erweiterte Pfad auf die schrittweise Erweiterung von Funktionsumfang, Reichweite und organisatorischer Verankerung. Im Zentrum stehen dabei insbesondere Multi-Site-Föderation, der strukturierte Einsatz von Hardware-in-the-Loop-(HIL-)Komponenten, der Ausbau von Governance- und Compliance-Mechanismen sowie die Skalierung der Plattform hinsichtlich Szenariokatalog, Nutzerzahlen und Betriebsmodellen.

Aus architektonischer Perspektive dient der 12-Monats-Pfad dazu, die in den Referenzarchitekturen A und B angelegten Fähigkeiten – etwa Föderationskonzepte, Interoperabilitätsmechanismen, Observability- und Sicherheitsarchitektur – von einer initialen, lokal fokussierten Nutzung in Richtung eines organisations- oder standortübergreifenden Einsatzes zu entwickeln. Dies umfasst typischerweise den Übergang von monolithisch organisierten Übungsumgebungen zu verteilten, miteinander gekoppelten Trainingslandschaften, in denen Szenarien, Ressourcen und Telemetriedaten zwischen Standorten oder Organisationseinheiten koordiniert und ausgetauscht werden können, ohne die definierten Sicherheits- und Governance-Richtlinien zu unterlaufen. Organisatorisch ist der erweiterte Pfad als Transformationsphase zu verstehen, in der die Plattform von einem primär technischen Vorhaben zu einem integralen Bestandteil der Ausbildungs-, Übungs- und ggf. Einsatzvorbereitungsprozesse wird. Dies setzt voraus, dass Governance-Prozesse (z. B. für Szenario-Lifecycle, Freigaben, Änderungen und AAR-Auswertung) verstetigt, Rollen- und Verantwortlichkeitsstrukturen geschärft und Schnittstellen zu bestehenden Planungs-, Ausbildungs- und Berichtssystemen etabliert werden. Gleichzeitig müssen Skalierungsfragen – etwa im Hinblick auf parallele Übungsreihen, unterschiedliche Nutzergruppen, abgestufte Sicherheitsdomänen und Betrieb über mehrere Standorte hinweg – systematisch adressiert werden.

Die nachfolgenden Unterkapitel konkretisieren diesen erweiterten Pfad in Form von Phasen, die exemplarisch einen Horizont von rund zwölf Monaten abdecken. Sie beschreiben, wie aufbauend auf dem MVP schrittweise zusätzliche Szenarien und Trainingsformate integriert, föderierte und HIL-gestützte Einsatzszenarien vorbereitet und in den Betrieb überführt, Governance- und Compliance-Mechanismen ausgebaut und technische wie organisatorische Skalierungsaspekte adressiert werden. Damit bildet der erweiterte Pfad die Brücke zwischen der initialen Inbetriebnahme und einem Zielzustand, in dem die Trainingsplattform als dauerhaft etablierte, auditierbare und weiterentwickelbare Infrastruktur im Regelbetrieb verankert ist.

4.12.3.1 Phase 4 (Monat 6–9): Ausbau Szenariokatalog & Föderationsfähigkeit

In Phase 4 wird der Fokus vom primär lokal ausgerichteten MVP-Betrieb hin zu einer erweiterten Nutzung der Plattform als organisationsübergreifendes Trainingsinstrument verschoben. Im Mittelpunkt stehen der systematische Ausbau des Szenariokatalogs sowie die schrittweise Operationalisierung von Föderationsmechanismen. Ziel ist es, die Plattform dahin zu entwickeln, dass sie nicht nur einzelne Referenzszenarien abbildet, sondern ein breiteres Spektrum an Trainingsformaten unterstützt und erste, kontrollierte Multi-Site-Übungen mit gemeinsamen Auswertungsstrukturen ermöglicht.

Schwerpunkte

- Erweiterung des Szenariokatalogs: In einem ersten Schwerpunkt wird der bestehende Szenariokatalog über die bislang implementierten Referenzszenarien hinaus erweitert. Dies umfasst insbesondere:
 - zusätzliche Cyber-Range-Szenarien, die unterschiedliche Angriffs- und Verteidigungsprofile, Eskalationsstufen und Komplexitätsgrade adressieren,

- Guided Labs, in denen Lernpfade stärker geführt und mit didaktischen Hilfestellungen (Hinweisen, Zwischenchecks, automatisierten Feedbacks) angereichert werden,
 - kombinierte Übungen, beispielsweise Blue-Team-Übungen, bei denen Teilnehmende über mehrere Rollen hinweg zusammenarbeiten und in denen ggf. föderierte Partner-Sites eingebunden werden.
 - Die Erweiterung des Katalogs erfolgt nicht rein quantitativ, sondern entlang definierter Lernziele und Kompetenzstufen. Szenarien werden mit Metadaten (z. B. Schwierigkeitsgrad, benötigte Ressourcen, Sicherheitsdomäne, Abhängigkeiten zu Föderations- oder HIL-Funktionen) versehen, um Planung, Zuweisung und Auswertung zu unterstützen. Damit bildet der Szenariokatalog zunehmend die Rolle eines zentralen „Produktportfolios“ der Trainingsplattform.
- Operationalisierung der Föderationslinks: Ein zweiter Schwerpunkt liegt auf der schrittweisen Operationalisierung der in der Architektur vorgesehenen Föderationsmechanismen. Dies umfasst insbesondere:
 - die Definition und Umsetzung von Austauschprofilen, in denen festgelegt wird, welche Informationen über Föderationsgrenzen hinweg ausgetauscht werden dürfen und in welcher Form. Typische Profile betreffen etwa Telemetriedaten und AAR-relevante Informationen (z. B. selektive Metriken und Ereignisse), die Abbildung von Namensräumen und VRFs zwischen Sites sowie Mechanismen zur Datenminimierung (z. B. Pseudonymisierung, Aggregation, Filterregeln),
 - die Durchführung erster föderierter Pilotübungen, bei denen mindestens zwei Sites – z. B. ein zentrales Übungszentrum und ein Partnerstandort – gemeinsam an einem abgestimmten Szenario teilnehmen. Für diese Pilotübungen werden gemeinsame AAR-Timelines etabliert, sodass Ereignisse, Telemetrie und Entscheidungszeitpunkte über Standorte hinweg konsistent ausgewertet werden können.
 - Die Pilotübungen dienen dazu, technische und organisatorische Fragestellungen der Föderation unter kontrollierten Bedingungen zu klären (z. B. Latenz- und Bandbreitenanforderungen, Abstimmung von Rollen und Verantwortlichkeiten, Freigabe- und Abbruchmechanismen) und daraus belastbare Muster für spätere, breiter ausgerollte Föderationsszenarien abzuleiten.
 - Etablierung von Governance-Prozessen: Parallel zum funktionalen Ausbau werden in Phase 4 Governance-Prozesse verankert, die die Qualität, Sicherheit und Nachvollziehbarkeit des erweiterten Betriebs sicherstellen. Dies betrifft insbesondere:
 - Prozesse zur Szenario-Freigabe, in denen neue oder geänderte Szenarien vor ihrem Einsatz hinsichtlich technischer Integrität, didaktischer Eignung und Sicherheitsanforderungen überprüft und dokumentiert freigegeben werden,
 - Verfahren für den Aufbau und die Änderung von Föderationslinks, einschließlich standardisierter Vereinbarungen zu Austauschprofilen, Sicherheitszielen, Verantwortlichkeiten und Abnahmebedingungen,
 - Mechanismen der Änderungskontrolle (Change Management), in denen wichtige Architektur- und Betriebsentscheidungen in Form von ADRs

dokumentiert, Versionierungsketten nachvollziehbar abgebildet und Freigaben mindestens nach dem Vier-Augen-Prinzip erteilt werden.

- Diese Governance-Prozesse werden eng mit den bestehenden Werkzeugen und Artefakten (z. B. Repositories, Pipelines, Policy- und Konfigurationsmanagement) verzahnt, sodass Freigaben und Änderungen nicht nur organisatorisch, sondern auch technisch nachvollziehbar umgesetzt werden können.

Ergebnis: Mit Abschluss der Phase 4 liegt eine Trainingsplattform vor, die über einen deutlich erweiterten Szenariokatalog verfügt und erste, kontrollierte föderierte Übungen unterstützt. Die Fähigkeit zur Multi-Site-Zusammenarbeit ist technisch erprobt und organisatorisch durch Governance-Prozesse abgesichert. Damit ist eine wesentliche Voraussetzung geschaffen, um in der folgenden Phase den Einsatz von HIL-Komponenten, die Skalierung auf höhere Lastprofile sowie die Verstetigung der Plattform im Regelbetrieb weiter voranzutreiben.

4.12.3.2 Phase 5 (Monat 9–12): HIL-Integration, Skalierung & Optimierung

In Phase 5 wird die Plattform von einer erweiterten, föderationsfähigen Trainingsumgebung zu einem nahezu voll ausgebauten Zielbild weiterentwickelt. Aufbauend auf dem erweiterten Szenariokatalog und den ersten föderierten Übungen rücken nun insbesondere drei Aspekte in den Vordergrund: die schrittweise Integration von Hardware-in-the-Loop-(HIL-)Komponenten, die Skalierung auf höhere Last- und Nutzungsszenarien sowie die institutionalisierte Nutzung von Erfahrungswissen und Telemetriedaten im Sinne eines kontinuierlichen Verbesserungsprozesses. Flankierend wird die Vorbereitung einer zweiten Site betrachtet, um die Plattform perspektivisch als verteiltes System mit klar geregelten Betriebs- und Wiederanlaufkonzepten betreiben zu können.

Schrittweise Integration von Hardware-in-the-Loop (HIL)

Ein zentraler Schritt dieser Phase ist die kontrollierte Integration realer Hardwarekomponenten in die Trainingsplattform. Die Anbindung von HIL erfolgt schrittweise und ausschließlich über spezifizierte Adapter und Guard-Komponenten, die sowohl funktionale als auch sicherheitsbezogene Anforderungen abdecken.

- Auf technischer Ebene werden Schnittstellen beschrieben, über die physische Systeme (z. B. spezialisierte Appliances, Hardware-Sensorik, industrielle Steuerungen) mit simulations- oder szenariobasierten Komponenten der Plattform interagieren können.
- Guard-Komponenten übernehmen die Aufgabe, die Kommunikationspfade zwischen Plattform und HIL-Geräten zu überwachen, zu filtern und – sofern erforderlich – zu begrenzen, um ungewollte Seiteneffekte oder sicherheitskritische Zustände zu vermeiden.
- Die Qualität der HIL-Integration wird durch Positiv- und Negativtests validiert:
- Positivtests prüfen, ob definierte, zulässige Interaktionen erwartungsgemäß funktionieren (z. B. korrekte Umsetzung von Szenarioereignissen in HIL-Verhalten und umgekehrt).
- Negativtests stellen sicher, dass unzulässige oder fehlerhafte Aktionen – etwa Verstöße gegen Policies, unerwartete Konfigurationsänderungen oder unautorisierte Zugriffe – zuverlässig erkannt, blockiert und in den relevanten Observability- und Audit-Sichten abgebildet werden.

Dadurch wird gewährleistet, dass die HIL-Integration nicht nur technisch funktionsfähig, sondern auch aus Sicherheits- und Governance-Sicht belastbar ist.

Skalierung und Feintuning von Kapazitätsplanung und Ressourcennutzung

Parallel zur HIL-Integration wird die Plattform auf höhere Lastprofile und größere Nutzerzahlen skaliert. Ziel ist es, die in den vorangegangenen Phasen etablierten Mechanismen so zu erweitern und zu justieren, dass auch mehr parallele Runs, größere Teilnehmerzahlen und komplexere Szenarien stabil unterstützt werden können.

- Es werden Last- und Stresstests durchgeführt, die gezielt auf typische Spitzenbelastungen zugeschnitten sind (z. B. gleichzeitige Startphasen mehrerer Übungen, parallele Auswertungen und AAR-Erstellung, föderierte Szenarien mit mehreren Sites).
- Auf Basis dieser Tests werden Kapazitätsmodelle für Compute-, Speicher- und Netzressourcen verfeinert und in konkrete Planungs- und Skalierungsrichtlinien überführt (z. B. Cluster-Größen, Ressourcenkontingente pro Szenario, Reserven für Spitzenlast).
- Je nach gewählter Referenzarchitektur werden Mechanismen wie Cluster-Skalierung, Ressourcenkontingente und Priorisierung (bei Architekturen mit Kubernetes) beziehungsweise VM-Pools, Snapshot-Strategien und Host-Sizing (bei VM-zentrierten Architekturen) optimiert und in Runbooks überführt.

Das Zusammenspiel von Observability-Daten, Lasttest-Ergebnissen und SLO-Überwachung ermöglicht ein zielgerichtetes Feintuning der Ressourcennutzung, sodass sowohl Überlastsituationen als auch ineffiziente Überprovisionierung schrittweise reduziert werden können.

Aufbau eines kontinuierlichen Verbesserungsprozesses (KVP)

Ein weiterer Kernbaustein dieser Phase ist der Aufbau eines kontinuierlichen Verbesserungsprozesses, der sicherstellt, dass Erkenntnisse aus dem laufenden Betrieb systematisch in die Weiterentwicklung der Plattform einfließen.

- Daten aus AARs und Telemetrie (Metriken, Events, Logs, Traces) werden gezielt ausgewertet, um Muster zu erkennen – etwa wiederkehrende Engpässe, typische Fehlerbilder oder didaktisch besonders wirksame Szenariokonstellationen.
- Auf dieser Grundlage werden Lessons Learned dokumentiert und in Form konkreter Maßnahmen in den Plattformbetrieb zurückgespielt, etwa durch:
 - die Anpassung oder Ergänzung von Sicherheits- und Betriebs-Policies,
 - die Weiterentwicklung und Priorisierung des Szenariokatalogs (z. B. stärkere Ausprägung häufig nachgefragter Kompetenzbereiche),
 - die Aktualisierung von Architekturentscheidungen (ADRs), sofern sich geänderte Rahmenbedingungen oder neue Erkenntnisse ergeben.

Der KVP verknüpft damit technische, organisatorische und didaktische Perspektiven: Architektur, Betrieb und Trainingskonzepte werden nicht als statische Ergebnisse verstanden, sondern als kontinuierlich zu justierende Systembestandteile, die sich an beobachteten Effekten und Rückmeldungen ausrichten.

Vorbereitung einer zweiten Site und Betriebs-/DR-Konzepte

Schließlich wird in Phase 5 die Vorbereitung einer möglichen zweiten Site vorangetrieben. Dies kann beispielsweise eine Trennung zwischen einem zentralen Übungszentrum und einem oder mehreren Schulungsstandorten sein.



- Es werden Szenarien und Betriebsmodelle entwickelt, in denen Aufgaben und Rollen auf mehrere Standorte verteilt sind (z. B. zentrale Plattform-Administration und dezentrale Trainingsdurchführung).
- Daraus abgeleitet entstehen Betriebskonzepte für Multi-Site-Setups, inklusive Zuständigkeitsregelungen, Kommunikations- und Eskalationspfaden, sowie
- Disaster-Recovery-(DR-)Konzepte, die Fragen der Wiederanlaufreihenfolge, Datenreplikation, Failover-Strategien und der Wiederherstellung kritischer Dienste über Standorte hinweg adressieren.

Diese Vorarbeiten schaffen die Grundlage dafür, die Plattform perspektivisch als verteiltes System mit redundanten und georedundanten Anteilen betreiben zu können, ohne die in den früheren Kapiteln definierten Sicherheits- und Governance-Anforderungen zu unterlaufen.

Mit Abschluss der Phase 5 liegt eine Trainingsplattform vor, die dem erweiterten Zielbild sehr nahekommt:

- föderierte Übungen mit mindestens einem Partner- bzw. Zweitstandort sind technisch und organisatorisch etabliert,
- HIL-Komponenten sind über spezifizierte, getestete Adapter und Guards eingebunden,
- die Plattform ist auf skalierte Trainingsprogramme mit höheren Lastprofilen ausgelegt,
- Governance, KVP und Betriebs-/DR-Konzepte sind organisatorisch verankert.

Damit ist die Trainingsplattform nicht mehr nur ein lokales, technisch ausgerichtetes Projekt, sondern eine dauerhaft etablierte Infrastruktur, die in die Ausbildungs- und Übungsprozesse der Organisation eingebettet ist und sich auf Basis messbarer Daten und strukturierter Rückkopplung kontinuierlich weiterentwickeln lässt.

4.12.4 Einführungs- und Migrationsplan

Die Einführung der Trainingsplattform erfolgt nicht als isolierter Technik-Rollout, sondern als gesteuerte Transformation einer bestehenden Übungslandschaft in ein neues, stärker automatisiertes, observables und auditierbares Zielbild. In den allermeisten Organisationen existieren bereits gewachsene Trainingsumgebungen, Szenarien und Unterstützungsprozesse – von manuell aufgebauten Labors über ad-hoc-Skripte bis hin zu eigenentwickelten Tools und Dokumentvorlagen. Ein Einführungs- und Migrationsplan muss diese Ausgangslage berücksichtigen und einen Pfad aufzeigen, der sowohl betriebliche Kontinuität als auch Lern- und Anpassungsfähigkeit sicherstellt. Vor diesem Hintergrund wird die Einführung der Plattform als phasenweiser Übergang bei paralleler Koexistenz von Alt- und Neuumgebung konzipiert. Anstelle eines „Big-Bang“-Wechsels, bei dem die bestehende Infrastruktur zu einem Stichtag vollständig abgelöst wird, sieht der Plan eine schrittweise Migration vor, in der beide Welten zunächst nebeneinander bestehen. Dies reduziert das Risiko, ermöglicht kontrollierte Pilotierungen und schafft den Raum, technische und didaktische Erfahrungen systematisch in die Weiterentwicklung der Plattform einfließen zu lassen. Im Folgenden werden fünf ineinandergreifende Schritte beschrieben: (1) Vorbereitung und Inventarisierung, (2) Koexistenzphase und Pilotierung, (3) schrittweise Migration des Szenariokatalogs, (4) Umstellung der Trainingsprozesse sowie (5) Ablösung bzw. Stilllegung von Altkomponenten. Die Schritte folgen einer logischen Abfolge, können in der praktischen Umsetzung jedoch teilweise überlappen und iterativ durchlaufen werden.

4.12.4.1 Vorbereitung und Inventarisierung

Die erste Phase dient der Systematisierung der Ausgangslage. Ziel ist, ein hinreichend präzises Bild der bestehenden Übungslandschaft zu gewinnen, um sinnvolle Startpunkte für die Migration bestimmen und spätere Abhängigkeiten besser einschätzen zu können. Hierzu werden zunächst die vorhandenen Trainingsumgebungen und Szenarien erfasst. Dies umfasst technische Aspekte (z. B. genutzte Netz- und Systemtopologien, eingesetzte Tools, Automatisierungsgrad) ebenso wie didaktische Dimensionen (Lernziele, Zielgruppen, typische Einsatzfrequenz, Abhängigkeiten zu Prüfungsordnungen oder Zertifizierungsanforderungen). Auch informelle oder „inoffizielle“ Lösungen – etwa von einzelnen Trainer:innen gepflegte Skripte, virtuelle Maschinen oder eigene Toolchains – sollten bewusst einbezogen werden, da sie häufig kritische Wissens Elemente enthalten und real genutzte Praxis abbilden. Parallel dazu wird die Unterstützungs- und Prozesslandschaft betrachtet: Wie werden Trainings geplant, vorbereitet, durchgeführt und nachbereitet? Gibt es etablierte AAR-Formate, Evaluationen, Qualitätszirkel? Welche Rollen (z. B. Übungsleitung, Trainer:in, technische Unterstützung, Planung) sind beteiligt, und wie verteilen sich Verantwortlichkeiten?

Auf Grundlage dieser Bestandsaufnahme werden Szenarien identifiziert, die sich als Startkollektion für die neue Plattform eignen. Typischerweise handelt es sich hierbei um Trainings,

- die einen hohen didaktischen Mehrwert besitzen („High-Value-Trainings“)
- die wiederkehrend durchgeführt werden und damit von Reproduzierbarkeit und Automatisierung besonders profitieren,
- deren technische Komplexität beherrschbar ist, sodass sie sich für eine erste Umsetzung im neuen Szenariomodell eignen,
- und die organisatorisch gut abgegrenzt werden können (z. B. bestimmte Kurse, Jahrgänge oder interne Trainingsformate).

Das Ergebnis der Vorbereitungs- und Inventarisierungsphase ist ein strukturierter Überblick über die bestehende Übungslandschaft und eine priorisierte Liste von Szenarien, die als erste auf die neue Plattform migriert werden sollen. Gleichzeitig werden erste Hypothesen darüber formuliert, welche Teile der alten Infrastruktur sich längerfristig erhalten lassen und welche mittelfristig ersetzt werden können.

4.12.4.2 Koexistenzphase und Pilotierung

Aufbauend auf dieser Vorbereitung beginnt die eigentliche Koexistenzphase, in der die neue Plattform in einem begrenzten Rahmen produktiv erprobt wird, während die Altumgebung den bestehenden Trainingsbetrieb absichert. Ziel ist es, die neue Architektur unter realen Bedingungen zu testen, ohne die Verfügbarkeit der bisherigen Trainingsangebote zu gefährden. In dieser Phase werden ausgewählte Trainingskohorten oder Nutzungskontexte systematisch auf die neue Plattform umgestellt. Beispielsweise kann ein bestimmter Kurs, eine definierte Zielgruppe oder ein einzelnes Modul zunächst exklusiv auf der neuen Plattform abgebildet werden, während andere Trainings weiterhin auf der Altumgebung laufen. Auf diese Weise lassen sich technische Stabilität, Usability und AAR-Qualität realitätsnah evaluieren, ohne dass bei Problemen der gesamte Trainingsbetrieb beeinträchtigt wäre. Ein besonderer Fokus liegt dabei auf der Erfahrung der Nutzer:innen. Trainer:innen, Übungsleitungen und Teilnehmende werden frühzeitig in Feedbackschleifen eingebunden. Neben objektiven Kennzahlen (z. B. Provisionierungszeiten, Fehlerraten, Anzahl erfolgreicher Durchläufe) werden subjektive Wahrnehmungen erhoben: Wie intuitiv sind die Oberflächen und Abläufe? Wie gut lassen sich Szenarien vorbereiten und variieren? Wie hilfreich und rechtzeitig sind Auswertungen und AARs?

Aus Sicht der Plattformbetreiber:innen dient die Koexistenzphase dazu,

- Betriebsprozesse im Kleinen zu erproben (z. B. Runbooks, Incident-Prozesse, Umgang mit Artefakt-Updates),
- die Integration in bestehende Umgebungen zu testen (z. B. Nutzerverzeichnisse, Ticketing, Reporting),
- und typische Fehlerbilder und Engpässe zu identifizieren (z. B. Limits bei Kapazität, Netzpfade, Rechte- und Rollenkonfiguration).

Die Koexistenzphase endet nicht mit einem einmaligen „Go“ oder „No-Go“, sondern mündet schrittweise in eine breitere Nutzung, sobald die Plattform für den gewählten Scope als stabil und ausreichend reif bewertet wird. Die Altumgebung bleibt in dieser Phase bewusst weiter verfügbar, insbesondere für kritische und hochsicherheitsrelevante Trainings, bis ausreichend Vertrauen in den neuen Betrieb besteht.

4.12.4.3 *Schrittweise Migration des Szenariokatalogs*

Nach einer erfolgreichen Pilotierung und stabilisiertem Betrieb im initialen Scope beginnt die Phase der schrittweisen Migration des Szenariokatalogs. Kernidee ist, bestehende Szenarien iterativ in das neue, deklarative Szenariomodell zu überführen, statt sie 1:1 technisch zu kopieren. Dabei werden die ausgewählten Szenarien zunächst in ihrer fachlichen Struktur modelliert: Zielsetzungen, Rollen, Phasen, Ereignisse, Bewertungskriterien und Abhängigkeiten zu Infrastrukturkomponenten werden explizit gemacht. Anschließend erfolgt die Überführung in das Everything-as-Code-Paradigma der Plattform. Dies umfasst die Abbildung der Szenarien in Form von deklarativen Beschreibungen, Templates und Artefakten, die versioniert, signiert und automatisiert validiert werden können.

Relevante Schritte sind insbesondere:

- Erstellung und Pflege von Szenariodefinitionsdateien,
- Zuordnung zu Infrastruktur- und Plattformbausteinen (z. B. Netze, Systeme, Dienste, Policies),
- Definition von Orchestrierungslogik (Start-/Reset-Pfade, Event-Injection, AAR-Hooks),
- und Ausgestaltung von Test- und Validierungsprozeduren, mit denen Szenarien vor dem produktiven Einsatz überprüft werden können.

Die Migration erfolgt priorisiert nach didaktischem Nutzen und technischer Komplexität. Szenarien mit hohem Mehrwert und überschaubarer Komplexität werden frühzeitig migriert, da hier der Nutzen des neuen Plattformansatzes schnell sichtbar wird. Kritische oder technisch besonders anspruchsvolle Szenarien – etwa solche mit umfangreicher Echtwelt-Integration, komplexen Schachtelungen oder hohen Sicherheitsanforderungen – werden bewusst später adressiert, wenn das Betriebsmodell der Plattform bereits stabil ist und genügend Erfahrungswerte aus weniger kritischen Fällen vorliegen. Während dieser Phase wird der Szenariokatalog nach und nach von der alten auf die neue Plattform „überhoben“, ohne dass zu einem festen Zeitpunkt alle Alt-Szenarien gleichzeitig abgeschaltet werden müssen. Es ist explizit vorgesehen, dass bestimmte Szenarien über einen längeren Zeitraum in beiden Welten parallel existieren, bis eine vollständige funktionale und organisatorische Gleichwertigkeit bzw. Überlegenheit der neuen Umsetzung erreicht ist.

4.12.4.4 *Umstellung der Trainingsprozesse*

Mit zunehmender Verlagerung des Szenariokatalogs auf die neue Plattform wird deutlich, dass nicht nur technische Artefakte, sondern auch Prozesse und Rollen angepasst werden müssen. Die Umstellung der Trainingsprozesse ist daher eine eigenständige, aber mit der Szenariomigration eng verzahnte Phase. Im Zentrum steht die Anpassung von Planungs-, Durchführungs- und Nachbereitungsprozessen an die neuen Werkzeuge und Möglichkeiten. Planungsprozesse müssen künftig auf den Szenariokatalog, die Orchestrierungsfunktionen und die Observability-Dashboards zugreifen können. Dies betrifft z. B. die Auswahl geeigneter Szenarien pro Zielgruppe, die frühzeitige Kapazitätsplanung für parallele Runs sowie die Koordination von Ressourcen und Rollen.

Während der Durchführung von Trainings verändern sich die Aufgabenprofile von Trainer:innen und Übungsleitungen:

- Statt manuell Systeme zu starten, zu konfigurieren oder zurückzusetzen, nutzen sie die Orchestrierungsfunktionen der Plattform, um Szenarien zu steuern.
- Fehlerbehebung und Support greifen auf telemetriegestützte Sichten zurück, statt ausschließlich auf individuelle Expertise und lokale Logs angewiesen zu sein.
- AARs werden zunehmend auf Basis strukturierter Daten und Dashboards erstellt, angereichert durch qualitative Beobachtungen, statt ausschließlich auf frei formulierten Erfahrungsberichten zu beruhen.

Um diese Veränderungen zu tragen, ist eine gezielte Qualifizierung der beteiligten Rollen notwendig. Trainer:innen, Übungsleitungen und unterstützende Technikteams werden in neuen Workflows, Oberflächen und Werkzeugen geschult. Ergänzend werden Runbooks und Checklisten erstellt, die typische Abläufe (z. B. Vorbereitung eines Trainings, Durchführung, Störungsbehebung, AAR-Erstellung) strukturiert und wiederholbar machen.

Die Umstellung der Trainingsprozesse ist damit keine rein technische, sondern eine organisationskulturelle Veränderung: Es verschiebt sich die Balance von individuell verantworteten, teils informellen Vorgehensweisen hin zu stärker standardisierten, datenbasierten und auditierbaren Abläufen. Ein professionelles Change-Management (inkl. Kommunikation, Schulung, Feedbackschleifen) ist daher ein zentraler Erfolgsfaktor dieser Phase.

4.12.4.5 *Ablösung und Stilllegung von Altkomponenten*

Erst wenn die neue Plattform für die relevanten Trainingsszenarien stabil im Regelbetrieb eingesetzt wird, beginnt die schrittweise Ablösung und Stilllegung von Altkomponenten. Ziel ist es, redundante oder technisch überholte Teile der Altumgebung zurückzubauen, ohne Funktionslücken, Compliance-Verstöße oder Wissensverluste zu erzeugen. Zunächst wird identifiziert, welche Komponenten der Altumgebung funktional durch die neue Plattform abgedeckt werden und welche darüber hinaus weiterhin benötigt werden – etwa weil sie noch nicht migrierte Szenarien unterstützen, aus regulatorischen Gründen archiviert werden müssen oder bestimmte Spezialfunktionen bereitstellen, die (noch) nicht in das neue Zielbild überführt wurden.

Für zurückzubauende Komponenten werden Abschalt- oder Rückbaupfade definiert. Diese umfassen technische Aspekte (z. B. Decommissioning von Servern, Rückgabe von Ressourcen, Entfernung von Zugängen) ebenso wie organisatorische Dimensionen (z. B. Anpassung von Betriebshandbüchern, Löschen oder Archivieren von Dokumentationen). Ein besonderer Schwerpunkt liegt auf der Erfüllung von Audit- und Nachweispflichten:



- Relevante Logs, Reports, Konfigurationsstände und AARs werden in geeigneter Form archiviert, bevor Systeme endgültig stillgelegt werden.
- Es wird dokumentiert, welche Systeme wann und in welchem Zustand abgeschaltet wurden, um spätere Nachfragen – etwa im Rahmen von Revisionen – beantworten zu können.

Dieser Rückbau wird ebenfalls phasenweise durchgeführt. Komponenten, die nur noch geringe Nutzung aufweisen und voll durch die neue Plattform ersetzt sind, werden früher stillgelegt; Komponenten mit kritischer Bedeutung oder hohem Archivwert werden länger vorgehalten. Im Ergebnis entsteht eine bereinigte Zielumgebung, in der die Trainingsplattform die zentrale Rolle für Planung, Durchführung und Auswertung von Übungen übernimmt, während die Altinfrastruktur auf das notwendige Minimum reduziert bzw. vollständig abgebaut wurde.

4.12.4.6 *Architekturspezifische Aspekte der Einführung (Referenzarchitekturen A und B)*

Die Grundlogik des Einführungs- und Migrationsplans ist referenzarchitekturneutral; sie lässt sich sowohl auf die VM-zentrierte Referenzarchitektur A als auch auf die cloud-native Referenzarchitektur B anwenden. Dennoch ergeben sich in der praktischen Umsetzung Unterschiede, die bei Planung und Ressourcenzuteilung berücksichtigt werden sollten.

Die Referenzarchitektur A erleichtert insbesondere die Migration bestehender VM-basierter Szenarien, da bestehende virtuelle Maschinen, Images und Skripte häufig mit vergleichsweise geringem Anpassungsaufwand in das neue Betriebsmodell überführt werden können. Die Umstellung konzentriert sich hier stärker auf Konsolidierung, Härtung und Automatisierung der vorhandenen Mechanismen (z. B. einheitliche Golden Images, standardisierte Snapshot- und Clone-Prozesse, zentrales Konfigurationsmanagement). Für Organisationen mit stark VM-geprägter Ausgangslage kann dies den Einstieg in die neue Plattform erheblich vereinfachen.

Die Referenzarchitektur B bietet darüber hinaus zusätzliche Potenziale für Automatisierung und Skalierung – etwa durch GitOps, deklarative Workloads, Service-Mesh-gestützte Sicherheitsmechanismen und flexible Ressourcenzuteilung. In der Einführungsphase gehen diese Vorteile jedoch mit höheren Anforderungen an Know-how und Prozessreife einher: Containerisierung, GitOps-Workflows, Policy-as-Code im Kubernetes-Kontext und Mesh-Operation erfordern zusätzliche Kompetenzen und klare organisatorische Verankerung. Der Migrationsplan muss daher ausreichend Raum für Kompetenzaufbau, Pilotierung und die schrittweise Übertragung von Verantwortung auf neue Rollen (z. B. Plattform-Engineering, GitOps-Ops) vorsehen.

In beiden Fällen bleibt der Grundsatz bestehen, dass die Einführung nicht primär als technisches Provisionierungsprojekt, sondern als Transformation von Trainings- und Governance-Prozessen verstanden werden sollte. Die hier beschriebene Kombination aus Inventarisierung, Koexistenz, schrittweiser Szenariomigration, Prozessumstellung und geplanter Stilllegung der Altumgebung bildet dabei den Rahmen, in dem dieser Wandel nachvollziehbar und risikokontrolliert vollzogen werden kann.

4.12.5 *Konsolidiertes Risiko-Register mit Gegenmaßnahmen*

Das in diesem Kapitel dargestellte Risiko-Register ergänzt die in den Kapiteln 4.5 (Referenzarchitektur A) und 4.6 (Referenzarchitektur B) ausgearbeiteten, architekturspezifischen Risikokataloge um eine programm- und transformationsbezogene Perspektive. Während die dort betrachteten Risiken sich primär auf technische Architekturentscheidungen, deren Nebenwirkungen und architekturnahe Betriebsaspekte beziehen (z. B. Komplexität bestimmter

Bausteine, technologische Lock-in-Effekte, spezifische Sicherheitsangriffsflächen), adressiert das konsolidierte Risiko-Register die Frage, welche Gefährdungen sich insbesondere im Verlauf der Einführung, Migration und Verstetigung der Plattform ergeben. Im Fokus stehen damit Risiken, die nicht allein aus einzelnen technischen Komponenten oder Mustern resultieren, sondern aus der Wechselwirkung von Technik, Organisation und Prozess: etwa unzureichender Kompetenzaufbau in den beteiligten Teams, Überforderung durch die gleichzeitige Einführung mehrerer neuer Paradigmen (Everything-as-Code, GitOps, Zero-Trust, Föderation, HIL), unklare Verantwortlichkeiten im Übergang von Projekt- zu Linienbetrieb, unzureichend gesteuerte Abhängigkeiten von Lieferketten oder externe Rahmenbedingungen (z. B. regulatorische Anforderungen, Freigabeprozesse). Diese Risiken sind typischerweise nicht auf eine einzelne Referenzarchitektur beschränkt, sondern können beide Varianten, VM-zentriert und cloud-native, in unterschiedlicher Ausprägung betreffen.

Das konsolidierte Risiko-Register verfolgt daher zwei Ziele:

- Es schafft eine gemeinsame, architekturübergreifende Sicht auf zentrale Transformationsrisiken, die unabhängig davon bestehen, ob Referenzarchitektur A oder B umgesetzt wird oder ob beide Varianten in einer Übergangszeit parallel betrachtet werden.
- Es verknüpft diese Risiken systematisch mit steuerbaren Gegenmaßnahmen und Governance-Mechanismen, die in den vorangegangenen Kapiteln angelegt wurden (z. B. ADRs, RACI-Modelle, Policies-as-Code, Test- und Validierungskonzepte, Roadmap-Phasen).

Damit wird deutlich, dass Risiken nicht abstrakt „benannt“, sondern in einem konkreten Steuerungsrahmen verortet werden: Jedes Risiko wird einer oder mehreren Einführungsphasen (Roadmap-Phasen, Migrationsschritte) zugeordnet, relevanten Rollen und Gremien zugewiesen und mit Maßnahmen verknüpft, die im Projekt- und später im Linienkontext tatsächlich umgesetzt werden können. Ein weiterer Zweck des Risiko-Registers besteht darin, die Abhängigkeiten zwischen technischen Entscheidungen und organisatorischen Konsequenzen transparent zu machen. So können beispielsweise Entscheidungen zugunsten der cloud-nativen Referenzarchitektur B – mit ihren zusätzlichen Potenzialen für Automatisierung und Skalierung – erhöhte Anforderungen an GitOps-, Container- und Mesh-Expertise mit sich bringen und damit spezifische Risiken im Kompetenz- und Ressourcenhaushalt der Organisation erzeugen. Umgekehrt kann eine primäre Ausrichtung auf die VM-zentrierte Referenzarchitektur A zwar einen erleichterten Einstieg ermöglichen, aber langfristig Risiken in Bezug auf Skalierbarkeit, Effizienz oder Modernisierungsfähigkeit bergen. Das konsolidierte Risiko-Register hilft, solche Trade-offs im Einführungs- und Betriebsverlauf bewusst zu adressieren und nicht nur im reinen Architekturvergleich (Kapitel 4.7) zu betrachten. Strukturell ist das Risiko-Register so aufgebaut, dass jedes Risiko durch eine knappe Beschreibung, eine Einschätzung wesentlicher Auswirkungstypen (z. B. Termin, Kosten, Qualität, Sicherheit, Compliance), eine qualitative Bewertung von Eintrittswahrscheinlichkeit und Schadenshöhe sowie eine Reihe von präventiven und reaktiven Gegenmaßnahmen charakterisiert wird. Wo sinnvoll, wird der Bezug zu konkreten Roadmap-Phasen, Architekturentscheidungen oder Governance-Artefakten hergestellt (z. B. „Maßnahme durchzusetzen über ADR-Prozess“, „Monitoring über definierte Telemetrie-Kennzahlen“, „Verankerung in Schulungsplan“). Das Register ist explizit als lebendes Artefakt konzipiert: Es soll im Projektverlauf fortlaufend überprüft, ergänzt und im Übergang in den Regelbetrieb an die Linienorganisation übergeben werden. Die nachfolgenden Abschnitte listen exemplarisch zentrale Transformationsrisiken auf, die typischerweise im Rahmen der Einführung einer Trainingsplattform dieser Art auftreten, und skizzieren jeweils geeignete Gegenmaßnahmen. Sie bilden damit die Brücke zwischen der in diesem Kapitel beschriebenen Roadmap, dem Einführungs- und Migrationsplan und den architekturenspezifischen Risikobetrachtungen und

unterstützen die Organisation dabei, die Plattform nicht nur technisch erfolgreich aufzubauen, sondern auch unter Risiko- und Governance-Gesichtspunkten nachhaltig zu betreiben.

4.12.5.1 R-P1 – Komplexität & Ressourcenknappheit

Dieses Risiko adressiert die Gefahr, dass der Gesamtumfang der Plattform – mit ihren Funktionsblöcken Cyber-Range, Föderation, HIL-Integration sowie den Paradigmen Everything-as-Code und Zero-Trust – die tatsächlich verfügbaren personellen und zeitlichen Ressourcen übersteigt. Besonders in der Einführungsphase besteht die Möglichkeit, dass zu viele Teilaspekte gleichzeitig angegangen werden sollen (z. B. Aufbau der Infrastruktur, Szenariomigration, Föderation, HIL, Governance), ohne dass hierfür eine ausreichende personelle Ausstattung, ein realistischer Zeitplan oder eine klare Priorisierung vorliegt. In der Folge drohen Überlastung der beteiligten Teams, ständige Kontextwechsel und ein schleichender Aufbau technischer Schulden.

Die Auswirkungen zeigen sich typischerweise in Projektverzögerungen, unvollständig gehärteten Komponenten, halb eingeführten Prozessen und einer Plattform, die zwar konzeptionell vorgesehen ist, in der Praxis aber nur eingeschränkt und fehleranfällig nutzbar ist. Es besteht zudem das Risiko, dass die Organisation das Vorhaben als „zu komplex“ wahrnimmt und Vertrauen in die Tragfähigkeit der Architektur verliert, bevor der Mehrwert voll sichtbar geworden ist.

Gegenmaßnahmen zielen auf eine bewusste Reduktion und Fokussierung des Einführungsumfangs. Die strikte Ausrichtung auf einen klar begrenzten MVP-Scope entlang des 6-Monats-Pfads hilft, die Einführungsphase in überschaubare Pakete zu schneiden. Kritische Anforderungen – insbesondere im Bereich Sicherheit, Offline-/Air-Gap-Betrieb und Kerntrainings – werden systematisch vor Komfortfunktionen (zusätzliche Automatisierung, komplexe Visualisierungen, selten genutzte Szenariotypen) priorisiert. Erweiterungen in Richtung Föderation, HIL und breiter Szenariokatalog erfolgen phasenweise gemäß dem 12-Monats-Pfad, sobald technische und organisatorische Grundlagen stabil etabliert sind.

4.12.5.2 R-P2 – Skill-Gap für neue Betriebsmodelle

Die Einführung der Plattform erfordert Fähigkeiten, die über klassische Systemadministration deutlich hinausgehen: Infrastructure-as-Code/GitOps, Kubernetes/Service-Mesh-Betrieb, HLA/DDS-Föderation, Policies-as-Code und observability-getriebener Betrieb. Wenn diese Kompetenzen in den beteiligten Teams nicht oder nur punktuell vorhanden sind, entsteht ein Skill-Gap, der die Umsetzung der Zielarchitektur substanziell erschweren kann.

Die unmittelbare Auswirkung solcher Lücken sind Fehlkonfigurationen, ineffiziente Workarounds und ein Betrieb, der stark von wenigen „Schlüsselpersonen“ oder externen Partnern abhängt. Dadurch erhöht sich die Anfälligkeit gegenüber Personalwechseln, und es entstehen Risiken für Stabilität und Sicherheit (z. B. falsch gesetzte Policies, unvollständig gehärtete Cluster, suboptimale GitOps-Pipelines). Zudem kann sich eine kulturelle Barriere entwickeln, wenn Teams die neuen Betriebsmodelle als zu abstrakt oder zu weit entfernt von ihrer bisherigen Praxis wahrnehmen.

Gegenmaßnahmen setzen auf gezielten Kompetenzaufbau und strukturiertes Wissensmanagement. Bereits früh in der Einführungsphase sollte ein kleines Kernteam mit vertiefter Expertise in den relevanten Themenfeldern aufgebaut werden, das als Träger und Multiplikator der neuen Betriebsmodelle fungiert. Dieses Kernteam arbeitet mit Referenz-Artefakten – etwa Beispiel-Pipelines, Beispiel-Policies, Referenz-Topologien –, die als „lebende Blaupausen“ für den weiteren Ausbau dienen. Ergänzend bieten sich Pairing- bzw. Shadowing-Ansätze an, bei denen Plattform-Engineering eng mit Trainer:innen und Operativteams zusammenarbeitet und so technische und didaktische Perspektiven zusammenführt.

4.12.5.3 R-P3 – Artefakt-Supply-Chain & Air-Gap-Robustheit

Die Plattform ist in hohem Maße von Artefakten abhängig: VM-Images, Container-Images, Pakete, Konfigurationen, Szenariobeschreibungen und Policies. Eine unsichere oder unzureichend gesteuerte Artefakt-Supply-Chain – etwa fehlende Signaturen, unvollständige SBOM-Informationen oder unklare Herkunft von Artefakten – stellt ein erhebliches Sicherheitsrisiko dar. Hinzu kommt die spezifische Anforderung, die Plattform in stark eingeschränkt angebotenen oder air-gap-ähnlichen Umgebungen betreiben zu können; unzureichend getestete Offline-/Disconnect-Szenarien können hier zu Betriebsstörungen führen.

Mögliche Auswirkungen reichen von Sicherheitsvorfällen durch kompromittierte Artefakte über unerwartete Abhängigkeiten von externen Ressourcen (z. B. Registry- oder Paketquellen) bis hin zu Ausfällen im Trainingsbetrieb, wenn Updates, Patches oder Szenariokomponenten im kritischen Moment nicht verfügbar sind. Dies untergräbt sowohl die technische Vertrauenswürdigkeit als auch die Akzeptanz der Plattform in sicherheitskritischen Kontexten.

Gegenmaßnahmen bestehen in der konsequenten Absicherung der Artefakt-Supply-Chain und der systematischen Erprobung von Offline-Betriebsszenarien. Dazu gehören die verpflichtende Nutzung von Signaturen und SBOMs für zentrale Artefakte, Quarantäne-Importe mit klar definierten Prüf- und Freigabeschritten sowie die Etablierung dokumentierter Promotionsprozesse (Quarantäne → Staging → Produktion). Regelmäßige Disconnect-Tests, deren Ergebnisse in Observability- und AAR-Artefakte einfließen, stellen sicher, dass die Plattform auch ohne externe Abhängigkeiten funktionsfähig bleibt und Importpfade im Fehlerfall Fail-Closed reagieren.

4.12.5.4 R-P4 – Föderations- und HIL-Risiken

Die Einführung von Föderationslinks und HIL-Adaptoren erweitert die Reichweite und Realitätsnähe der Trainingsplattform, erhöht aber zugleich ihre Komplexität und das Sicherheitsrisiko. Fehlkonfigurationen in diesem Bereich – etwa unklare oder durchlässige Namensraum-Isolation, unzureichend getestete Guards, fehlende Begrenzung der Datenflüsse – können zu Verletzungen von Mandantengrenzen, unerwünschtem Datenabfluss oder sicherheitsrelevanten Zwischenfällen führen.

Die Konsequenzen sind potenziell gravierend: Neben direkten Sicherheitsvorfällen drohen Vertrauensverlust bei Partnern, die an föderierten Übungen teilnehmen, und Zweifel an der Eignung der Plattform für hochkritische Szenarien. Insbesondere in HIL-Kontexten können Fehlkonfigurationen darüber hinaus physische Systeme beeinträchtigen, was zusätzliche Schutzmaßnahmen erforderlich macht.

Zur Begrenzung dieses Risikos ist eine gestufte Einführung zentral: Zunächst wird die Plattform als Single-Site-System stabilisiert, anschließend werden Föderationsmechanismen in klar begrenzten Pilotstrecken etabliert, und erst in einem weiteren Schritt erfolgt die Anbindung von HIL-Komponenten. Für alle Föderationslinks und HIL-Adaptionen sind standardisierte Test- und AbnahmeprozEDUREN vorzusehen, die Positiv- und Negativtests sowie, je nach Schutzbedarf, Penetrationstests umfassen. Ergänzend sollten klare „Kill-Switches“ und Runbooks für Sofort-Disconnects bei Policy-Verstößen oder sicherheitskritischen Ereignissen definiert werden, um im Ernstfall schnell und kontrolliert reagieren zu können.

4.12.5.5 R-P5 – Zeit- und Dateninkonsistenz

Die Qualität von AARs und die forensische Nachvollziehbarkeit von Trainingsverläufen hängen maßgeblich davon ab, dass Zeitbasis und Telemetrie konsistent sind. Inkonsistente Zeitquellen (z. B. divergierende NTP-Konfigurationen, unsauber synchronisierte Systeme) oder unvollständige

Telemetriedaten führen zu widersprüchlichen Ereigniszeitleisten, Lücken in der Beweisführung und eingeschränkter Aussagekraft von Auswertungen.

Die Auswirkungen reichen von erschwerter Nachweisführung gegenüber Prüfinstanzen (z. B. bei Audits oder Untersuchungen) über reduzierte didaktische Qualität der AARs bis hin zu Akzeptanzproblemen bei Stakeholdern, die sich auf verlässliche zeitliche Rekonstruktionen und Metriken verlassen müssen. In Extremfällen kann dies dazu führen, dass zentrale Ziele der Plattform – Transparenz, Reproduzierbarkeit und Belastbarkeit von Ergebnissen – nicht erreicht werden.

Gegenmaßnahmen setzen an der technischen und konzeptionellen Grundlage der Zeit- und Telemetrieerfassung an. Die durchgängige Nutzung einer lokal kontrollierten Zeitquelle und die Verknüpfung aller relevanten Ereignisse mit einer Run-ID stellen sicher, dass zeitliche Bezüge konsistent und rekonstruierbar bleiben. Zeitkonsistenz-Checks sowie Telemetrie-Vollständigkeitsmetriken werden in Observability-Dashboards verankert, sodass Abweichungen frühzeitig sichtbar sind. In AAR-Paketen sollten bekannte Timeline-Abweichungen explizit gekennzeichnet und analysiert werden, um eine transparente Interpretation der Ergebnisse zu ermöglichen und systematische Ursachen iterativ zu adressieren.

4.12.5.6 *R-P6 – Akzeptanz & didaktische Wirksamkeit*

Unabhängig von ihrem architektonischen Reifegrad kann die Plattform ihr Potenzial nur entfalten, wenn sie von Trainer:innen, Übungsleitungen und Teilnehmenden akzeptiert und als didaktisch wirksam erlebt wird. Wird die Plattform als zu komplex, zu „technolastig“ oder als bürokratische Hürde wahrgenommen, besteht die Gefahr, dass informelle Lösungen – etwa individuell gepflegte VMs, Skripte oder separate Tools – parallel weiter genutzt und die Plattform umgangen wird.

Die Konsequenz wäre eine geringe Nutzung der Plattform, eine fragmentierte Datenbasis für AARs und Governance sowie eine Diskrepanz zwischen dem intendierten Zielbild (zentralisierte, auditierbare Trainingsplattform) und der gelebten Praxis. Didaktisch kann dies dazu führen, dass Zeit und Aufmerksamkeit eher in das Bedienen der Plattform als in die Lerninhalte fließen oder dass die Plattform gerade in anspruchsvollen Szenarien gemieden wird.

Gegenmaßnahmen bestehen in der frühen und kontinuierlichen Einbindung der pädagogischen Rollen. Trainer:innen sollten bereits während PoC- und MVP-Iterationen beteiligt sein, Feedback geben und gemeinsam mit dem Plattformteam Usability-kritische Workflows gestalten. Besondere Aufmerksamkeit verdienen Abläufe, die für den Trainingsalltag zentral sind – etwa Start, Pause, Reset von Szenarien und AAR-Export – und idealerweise mit wenigen, klar nachvollziehbaren Interaktionen bedienbar sein müssen. Darüber hinaus sollte der Mehrwert der Plattform aktiv sichtbar gemacht werden, etwa durch deutlich verbesserte Reset-Zeiten, konsistente und reichhaltige AARs oder die Möglichkeit, Szenarien reproduzierbar in unterschiedlichen Kontexten einzusetzen.

4.12.5.7 *R-P7 – Governance- und Compliance-Lücken*

Die Plattform bewegt sich in einem Umfeld, in dem Architekturentscheidungen, Sicherheitsrichtlinien und Betriebsprozesse häufig auditierbaren Anforderungen unterliegen. Werden Entscheidungen, Policies und Änderungen nicht hinreichend dokumentiert, versioniert und an Verantwortlichkeiten gekoppelt, entstehen Governance- und Compliance-Lücken: Es ist dann nicht transparent, warum bestimmte Entscheidungen getroffen wurden, wer sie verantwortet und wie sie sich im Betrieb niederschlagen.

Die Auswirkungen können sich in Schwierigkeiten bei Audits, Unsicherheiten in der Entscheidungsfindung und einem inkonsistenten Betrieb äußern. Insbesondere bei sicherheits-

oder compliance-relevanten Fragestellungen (z. B. Umgang mit personenbezogenen Daten, Nachvollziehbarkeit von Zugriffen, Nachweis der Wirksamkeit von Kontrollen) kann dies zu erheblichen Problemen führen.

Gegenmaßnahmen zielen auf den Aufbau eines integrierten Governance-Rahmens. Zentral ist die systematische Nutzung von Architectural Decision Records (ADRs), in denen wichtige Architekturentscheidungen dokumentiert und mit Begründungen, Alternativen und Konsequenzen versehen werden. RACI-Modelle definieren Rollen und Verantwortlichkeiten klar, während Policies-as-Code eine technische Umsetzung und Prüfung von Richtlinien in Pipelines und Laufzeitumgebungen ermöglichen. Ergänzend sollte ein formal definierter Freigabeprozess für Szenarien, Policies und Releases etabliert werden, der mindestens eine Vier-Augen-Freigabe vorsieht. Governance-Artefakte werden mit Observability- und AAR-Evidenzen verzahnt, sodass Entscheidungsfolgen im Betrieb nachvollziehbar und überprüfbar sind.

4.12.5.8 R-P8 – Betriebs- und Supportkontinuität

Schließlich besteht das Risiko, dass zentrale Funktionen der Plattform zu stark an einzelne Personen gebunden sind oder dass Wissen über kritische Betriebsprozesse nur implizit und nicht in Runbooks, Automatisierung und Monitoring abgebildet ist. In solchen Fällen führen Abwesenheiten, Fluktuation oder organisatorische Umstrukturierungen schnell zu Wissensverlust, verlängerten Wiederanlaufzeiten und erhöhter Ausfallwahrscheinlichkeit.

Ein Mangel an dokumentierten und automatisierten Betriebsabläufen führt zudem dazu, dass Routineaufgaben (z. B. Provisionierung, Backups, Patch-Management) inkonsistent durchgeführt werden und Fehler häufiger unentdeckt bleiben. Dies wirkt sich direkt auf die Stabilität und Verfügbarkeit der Plattform aus und kann das Vertrauen der Nutzenden in ihre Zuverlässigkeit beeinträchtigen.

Gegenmaßnahmen zielen auf die Institutionalisierung von Betriebskompetenz. Zentrale Betriebsprozesse werden vollständig dokumentiert (Runbooks, DR-Drills, Rotationspläne) und, wo immer möglich, automatisiert (z. B. Provisionierung, Backups, Patch-Fenster). Regelmäßige Übungen – etwa Disaster-Recovery-Drills oder „Game Days“ – dienen dazu, die Belastbarkeit der Plattform und der Betriebsorganisation zu überprüfen und Schwachstellen frühzeitig aufzudecken. Durch Rotationen in Rufbereitschaften und Verantwortlichkeiten wird verhindert, dass kritisches Wissen bei Einzelnen konzentriert bleibt.

Das konsolidierte Risiko-Register bildet damit eine verbindende Struktur zwischen den in der Architektur beschriebenen Gestaltungsentscheidungen, der Roadmap zur Einführung und dem späteren operativen Betrieb der Trainingsplattform. Es ist explizit als lebendes Artefakt konzipiert, das im Verlauf der Einführung fortlaufend aktualisiert, um neu identifizierte Risiken ergänzt und regelmäßig mit den Erkenntnissen aus AARs, Observability und Betriebserfahrung abgeglichen wird. Auf diese Weise unterstützt es die Organisation dabei, die Plattform nicht nur technisch erfolgreich umzusetzen, sondern auch unter Risiko-, Governance- und Akzeptanzgesichtspunkten nachhaltig zu verankern.

5 Curriculum

Die Konzeption der Trainingsumgebung bestimmt die infrastrukturellen, technischen und architektonischen Voraussetzungen, unter denen das im Projekt Bumblebee entwickelte Ausbildungsprogramm realisierbar und belastbar umsetzbar wird. Sie definiert damit nicht nur die materiellen und funktionalen Rahmenbedingungen des Trainingsbetriebs, sondern auch jene sicherheitsbezogenen, betrieblichen und methodischen Anforderungen, die erfüllt sein müssen, damit cyberbezogene Lehr-/Lernprozesse in einer kontrollierten, reproduzierbaren und didaktisch nutzbaren Umgebung stattfinden können. Die Trainingsumgebung bildet insofern die technische Ermöglichungsstruktur des Gesamtvorhabens: Sie schafft den Handlungsraum, innerhalb dessen Szenarien modelliert, Übungen durchgeführt, Interaktionen beobachtet und Lernergebnisse in praxisnahen Kontexten erprobt werden können.

Darauf aufbauend konkretisiert das nachfolgende Curriculum, wie diese technischen und organisatorischen Voraussetzungen in ein systematisches Ausbildungsprogramm überführt werden, das auf nachhaltige Kompetenzentwicklung im militärischen Cyber- und Informationsraum ausgerichtet ist. Während die vorangegangenen Kapitel die Frage behandeln, unter welchen infrastrukturellen und architektonischen Bedingungen eine geeignete Trainingsumgebung bereitgestellt werden kann, richtet sich der Fokus des Curriculums auf die strukturierte Gestaltung der Qualifizierungsprozesse selbst. Im Zentrum steht damit nicht mehr primär die technische Ermöglichung von Ausbildung, sondern die fachliche, didaktische und organisatorische Ausformung eines Programms, das jene Wissensbestände, Fähigkeiten und Handlungskompetenzen adressiert, die für militärisches SOC- und NOC-Personal in sicherheitsrelevanten Einsatz- und Unterstützungskontexten erforderlich sind. Mit diesem Perspektivenwechsel verlagert sich die analytische Aufmerksamkeit von der Plattformlogik auf die Logik der Kompetenzentwicklung. Das Curriculum hat die Aufgabe, die in der Bedarfsanalyse identifizierten Anforderungen sowie die in der Trainingsumgebung geschaffenen Voraussetzungen in eine kohärente Ausbildungsarchitektur zu überführen. Es ordnet damit nicht lediglich einzelne Themenfelder oder Unterrichtsinhalte, sondern entwickelt einen systematischen Qualifizierungsrahmen, in dem fachliche Inhalte, Lernziele, didaktische Progression, Übungsformate und Evaluationslogiken aufeinander abgestimmt werden. Ein Curriculum in diesem Sinne ist nicht als bloße Zusammenstellung von Lehrgegenständen zu verstehen, sondern als strukturierendes Instrument, das festlegt, welche Kompetenzen in welcher Reihenfolge, auf welchem Anspruchsniveau und in welchen didaktischen Formaten aufgebaut, vertieft und überprüft werden sollen.

Im militärischen Cyberkontext besitzt eine solche curriculare Strukturierung besondere Relevanz, da die Anforderungen an Personal in SOC- und NOC-nahen Rollenprofilen nicht auf isoliertes technisches Spezialwissen reduziert werden können. Erforderlich ist vielmehr ein Kompetenzverständnis, das technisches Verständnis, analytische Urteilsfähigkeit, prozessuale Handlungssicherheit, organisationsbezogene Orientierung und kommunikative Anschlussfähigkeit in integrierter Form umfasst. Das Curriculum trägt diesem Umstand Rechnung, indem es nicht nur die Vermittlung cyberbezogener Fachinhalte adressiert, sondern deren systematische Einbettung in operative Abläufe, institutionelle Rahmenbedingungen und realitätsnahe Handlungssituationen. Es verfolgt damit einen Ansatz, in dem Wissensvermittlung, praktische Anwendung und reflexive Einordnung nicht nebeneinanderstehen, sondern als komplementäre Dimensionen militärischer Professionalisierung verstanden werden. Zugleich übernimmt das Curriculum eine vermittelnde Funktion zwischen den empirisch erhobenen Bedarfen des Projekts und ihrer konkreten didaktischen Umsetzung. Die Bedarfsanalyse hat gezeigt, dass ein wirksames Ausbildungsprogramm für militärisches SOC- und NOC-Personal sowohl grundlegende technische Kompetenzen als auch die Fähigkeit zur strukturierten Wahrnehmung, Bewertung, Dokumentation und Eskalation sicherheitsrelevanter Ereignisse fördern muss. Die Trainingsumgebung wiederum

definiert jene infrastrukturellen Voraussetzungen, unter denen solche Kompetenzen in praxisnahen, kontrollierten und sicherheitskonformen Settings entwickelt werden können. Das Curriculum bildet die Ebene, auf der beide Perspektiven zusammengeführt werden: Es übersetzt Bedarf in Lernziele, technische Möglichkeiten in didaktische Formate und konzeptionelle Anforderungen in eine nachvollziehbare Ausbildungsstruktur. Darüber hinaus ist das Curriculum als konzeptioneller Kernbereich des Gesamtberichts zu verstehen. In ihm verdichten sich die Ergebnisse der vorangegangenen Kapitel zu einem handlungsorientierten Ausbildungsmodell, das wissenschaftliche Fundierung und praktische Anschlussfähigkeit miteinander verbindet. Es schafft damit nicht nur einen Rahmen für die Auswahl und Strukturierung relevanter Wissensgebiete, sondern auch für die Bestimmung von Modulen, Progressionslogiken, Rollenbezügen und Formen der Kompetenzüberprüfung. Das Curriculum übernimmt somit eine doppelte Funktion: Einerseits systematisiert es die fachlichen und didaktischen Anforderungen des Ausbildungsfeldes, andererseits macht es sichtbar, wie diese Anforderungen unter Nutzung der entwickelten Trainingsumgebung in ein institutionell anschlussfähiges Ausbildungsprogramm überführt werden können.

Das nachfolgende Kapitel beschreibt das Curriculum daher nicht als isoliertes Teilprodukt, sondern als integratives Ordnungsmodell, in dem Bedarfsanalyse, Trainingsumgebung und Kompetenzentwicklung in einer gemeinsamen Entwicklungslogik zusammengeführt werden. Es legt dar, nach welchen Zielsetzungen, Strukturprinzipien und didaktischen Leitgedanken das Ausbildungsprogramm aufgebaut ist, welche Wissensgebiete und Module unterschieden werden, wie diese aufeinander bezogen sind und in welcher Weise daraus ein kohärenter Qualifizierungsrahmen für militärisches SOC- und NOC-Personal im Cyber- und Informationsraum entsteht. In dieser Perspektive bildet das Curriculum denjenigen Abschnitt des Gesamtberichts, in dem die technische Ermöglichungsstruktur des Vorhabens in eine wissenschaftlich fundierte und praxisorientierte Ausbildungsarchitektur überführt wird.

5.1 Scope & Abgrenzung des Curriculums

Dieses Curriculum definiert den fachlichen, didaktischen und organisatorischen Referenzrahmen für die Ausbildung militärischen Personals in Funktionen des Security Operations Center (SOC) und des Network Operations Center (NOC). Es beschreibt, welche Kompetenzen für diese Rollen erforderlich sind, wie sie in Wissensgebiete, Lernziele und Module übersetzt werden und nach welchen pädagogischen, methodischen und organisatorischen Prinzipien Ausbildung, Übung, Leistungsbewertung und Weiterentwicklung erfolgen sollen. Der Gegenstandsbereich geht damit bewusst über die Vermittlung technischer Fachinhalte hinaus und umfasst ebenso die lagebezogene Bewertung sicherheitsrelevanter Ereignisse, koordinierte Reaktion, adressatengerechte Kommunikation sowie die Einbindung cyberbezogener Erkenntnisse in Führungs-, Entscheidungs- und Eskalationsprozesse. Das Curriculum versteht Ausbildung folglich als Bestandteil eines übergeordneten Capability-Managements für den Cyber- und Informationsraum und als Brücke zwischen individueller Qualifizierung, organisationaler Einsatzbefähigung und langfristiger Fähigkeitsentwicklung.

Inhaltlich strukturiert sich das Curriculum in vier aufeinander aufbauende Ebenen. Erstens schafft eine Basisausbildung ein gemeinsames Fundament aus Begriffen, Konzepten und Denkmodellen, unter anderem zu Informationssicherheit, Risikomanagement, Resilienz, Identitäts- und Zugriffsmanagement, Klassifikation und sicherer Informationsverarbeitung. Zweitens werden gemeinsame operationelle Wissensgebiete vermittelt, die für SOC- und NOC-Personal gleichermaßen relevant sind, etwa Monitoring- und Alarmierungslogiken, Ereigniskorrelation, Incident Response, forensische Grundlagen, System- und Konfigurationsmanagement, Protokollanalyse sowie Methoden der Datenaufbereitung und Lageverdichtung. Drittens folgen rollenbezogene Vertiefungen mit detektions-, analyse- und lageorientierten Schwerpunkten im SOC sowie betriebs-, netzwerk- und OT-nahen Schwerpunkten im NOC. Viertens integriert das Curriculum Querschnittsthemen wie rechtliche und normative Rahmenbedingungen, ethische Verantwortung, Führungsbezug, Interoperabilität und kontinuierliche Professionalisierung. Damit wird militärische Handlungsfähigkeit im Cyber-Raum ganzheitlich adressiert, ohne operative Präzision und Umsetzbarkeit aus dem Blick zu verlieren.

Eine präzise inhaltliche Abgrenzung ist notwendig, um Reichweite und Anwendungslogik des Curriculums belastbar zu bestimmen. Nicht Gegenstand des Dokuments ist die vollständige Ausbildung sämtlicher Rollen des militärischen Cyber- und Informationsraums. Der Fokus liegt ausdrücklich auf defensiven, detektions-, analyse- und betriebsnahen Aufgabenprofilen von SOC- und NOC-Personal. Das Curriculum ist daher weder als Ausbildungsprogramm für offensive Cyberoperationen noch als Rahmenwerk für strategische Nachrichtengewinnung, allgemeine IT-Berufsausbildung, Softwareentwicklung oder die gesamthafte Ausbildung militärischer Führungs- und Stabsverwendungen konzipiert. Ebenso ersetzt es keine organisationsspezifischen technischen Einweisungen in konkrete Produkte, Plattformen oder proprietäre Werkzeuge. Solche Einweisungen bleiben erforderlich, sollen jedoch auf einem gemeinsamen, übertragbaren Kompetenzfundament aufbauen. Die Abgrenzung verhindert damit, dass Ausbildungsplanung von kurzfristigen Tool-Zyklen oder Herstellerlogiken dominiert wird, und sichert den Fokus auf nachhaltige Kompetenzentwicklung.

Auch der zeitliche und organisatorische Geltungsbereich des Curriculums ist bewusst offen, zugleich aber strukturell präzise gefasst. Das Dokument kann als geschlossene Lehrgangsarchitektur, als modulare Qualifizierungssequenz oder in Form kombinierter Präsenz-, Selbststudiums- und Übungsanteile umgesetzt werden. Auf eine starre Stundenplanung wird bewusst verzichtet; stattdessen beschreibt das Curriculum eine belastbare Struktur, die an nationale Verfügbarkeiten, Geheimschutzanforderungen, personelle Ressourcen, Infrastrukturbedingungen, Cyber-Range-Kapazitäten und bestehende militärische

Ausbildungskalender angepasst werden kann. Diese Offenheit ist keine konzeptionelle Unschärfe, sondern eine Designentscheidung zugunsten von Standardisierung und Adaptionfähigkeit unter heterogenen militärischen Rahmenbedingungen.

Von besonderer Bedeutung ist schließlich der normative und entwicklungsorientierte Charakter des Curriculums. Das Dokument erhebt nicht den Anspruch, alle gegenwärtigen und zukünftigen Technologien, Bedrohungsformen oder Organisationsmodelle vollständig vorwegzunehmen. Stattdessen definiert es einen belastbaren Kern aus Kompetenzen, Prinzipien, Ausbildungslogiken und Qualitätsanforderungen, der als stabiler Referenzrahmen dient und zugleich offen für regelmäßige Überprüfung, Anpassung und Erweiterung bleibt. Es ist insofern als lebendes Dokument zu verstehen, das an technologische Entwicklungen, veränderte Bedrohungslagen, neue regulatorische Anforderungen und gewonnene Einsatzerfahrungen rückgebunden werden muss. Gerade in einem hochdynamischen Operationsraum ist diese institutionalisierte Weiterentwicklung selbst Teil professioneller Qualitätssicherung.

Damit bestimmt das Curriculum sowohl seinen inhaltlichen Anspruch als auch seine bewusste Begrenzung. Es legt fest, welche Themen und Kompetenzen für die Qualifizierung von SOC- und NOC-Personal unverzichtbar sind, in welchen Bereichen vertiefte Spezialisierung erforderlich ist und welche Themenfelder bewusst außerhalb des Geltungsbereichs verbleiben. Gerade diese Klarheit in Bezug auf Reichweite, Schwerpunktsetzung und Abgrenzung ist eine wesentliche Voraussetzung für praktische Wirksamkeit, Anschlussfähigkeit an den Dienstbetrieb und zukünftige Weiterentwicklung.

5.2 Ausgangspunkt

Die Streitkräfte sind heute in hohem Maße von informations- und kommunikationstechnischen Systemen abhängig. Führungs- und Waffensysteme, Aufklärungs- und Kommunikationsmittel, logistische und infrastrukturelle Einrichtungen – sie alle bilden ein digitales Geflecht, das für Planung, Führung und Durchführung militärischer Operationen unverzichtbar ist. Cyberangriffe auf diese Systeme können die Einsatzbereitschaft, Entscheidungsfähigkeit und Handlungsfreiheit der Streitkräfte unmittelbar beeinträchtigen. Mit der zunehmenden Vernetzung entstehen neue Angriffsflächen, die von staatlichen und nichtstaatlichen Akteuren gezielt ausgenutzt werden. Neben klassischen Spionage- und Sabotageaktivitäten treten komplexe, mehrstufige Kampagnen, die über längere Zeiträume unentdeckt bleiben können. Security Operations Center (SOC) und Network Operations Center (NOC) übernehmen in diesem Umfeld eine Schlüsselrolle: Sie überwachen Netze und Systeme, erkennen und analysieren sicherheitsrelevante Ereignisse und unterstützen die militärische Führung bei der Bewertung der Cyber-Lage und der Einleitung von Gegenmaßnahmen.

Das vorliegende Curriculum beschreibt ein strukturiertes, mehrstufiges Ausbildungsprogramm für militärisches SOC- und NOC-Personal. Es schafft zunächst ein gemeinsames Grundlagenverständnis über Bedrohungen, Technologien und Prozesse und baut darauf spezialisierte Fähigkeiten für Betrieb, Detektion, Analyse und Reaktion auf. Die Inhalte sind modular aufgebaut und orientieren sich an Qualifikationsstufen, die vom grundlegenden Verständnis bis hin zur Expertenrolle im operativen Cyber- und Netzwerkbetrieb reichen. Neben den technischen Kenntnissen – etwa zu System- und Netzwerksicherheit, Logdatenanalyse, SIEM-Technologien, Vorfallbearbeitung und Forensik – berücksichtigt das Curriculum ausdrücklich auch organisatorische, rechtliche und ethische Rahmenbedingungen. Dazu gehören Rollen und Verantwortlichkeiten innerhalb der militärischen Führungsorganisation, Melde- und Entscheidungswege, nationale und internationale Vorgaben sowie Fragen von Informationssicherheit, Datenschutz, Geheimschutz und militärischer Ethik im Cyber-Raum. Praktische Übungen, Fallstudien und Szenarien auf Basis realistischer militärischer Lagen sorgen dafür, dass das Erlernte unmittelbar im Einsatz- und Übungsbetrieb anwendbar ist.

Ziel ist es, Angehörige der Streitkräfte systematisch zu befähigen, Cyberbedrohungen in Friedensbetrieb, Übungen und Einsätzen wirksam zu begegnen, Fehlentwicklungen frühzeitig zu erkennen und fundierte Gegenmaßnahmen einzuleiten. Gleichzeitig soll die Resilienz militärischer Systeme und Kommunikationsnetze erhöht und ihre Fähigkeit gestärkt werden, trotz Angriffen handlungsfähig zu bleiben („fight through“). Damit leistet das Curriculum einen wesentlichen Beitrag zur Sicherstellung der Führungs- und Einsatzfähigkeit der Streitkräfte im gesamten Einsatzspektrum – von der Landesverteidigung über Bündnisverpflichtungen bis hin zu internationalen Missionen.

5.3 Mission und Zielsetzung

Dieses Kapitel beschreibt den Auftrag und die übergeordneten Zielsetzungen des Ausbildungsprogramms für militärisches SOC- und NOC-Personal. Aufbauend auf der allgemeinen Einordnung in die sicherheitspolitischen und technologischen Rahmenbedingungen wird hier konkretisiert, welchen Beitrag das Curriculum zur Sicherstellung der Führungs- und Einsatzfähigkeit der Streitkräfte im Cyber- und Informationsraum leisten soll. Die Mission des Programms definiert dabei den grundsätzlichen Auftrag und Zweck der Ausbildung, während die Zielsetzungen die daraus abgeleiteten inhaltlichen Schwerpunkte und Wirkungsziele strukturieren. Sie bilden den Referenzrahmen für die Ausgestaltung der Module, Qualifikationsstufen und Lernziele und dienen zugleich als Grundlage für die spätere Evaluation der Wirksamkeit des Gesamtprogramms.

5.3.1 Mission des Ausbildungsprogramms

Die Mission dieses Ausbildungsprogramms besteht darin, Angehörige der Streitkräfte systematisch für die Aufgaben in einem militärischen Security Operations Center (SOC) und Network Operations Center (NOC) zu befähigen. Im Mittelpunkt steht die Fähigkeit, die Verfügbarkeit, Integrität und Vertraulichkeit militärischer Führungs-, Kommunikations- und Waffensysteme im gesamten Einsatzspektrum zu schützen und damit die Handlungsfähigkeit der Streitkräfte im Cyber- und Informationsraum dauerhaft sicherzustellen. SOC- und NOC-Personal soll in die Lage versetzt werden, sicherheitsrelevante Ereignisse in komplexen und stark vernetzten Umgebungen nicht nur technisch zu verstehen, sondern auch im Hinblick auf ihre operative Wirkung richtig einzuordnen und adäquate Maßnahmen abzuleiten.

Das Curriculum orientiert sich dabei an drei zentralen Leitgedanken. Erstens steht der Schutz der militärischen Handlungsfähigkeit im Vordergrund. Das Personal in SOC und NOC soll befähigt werden, Cyberangriffe und sicherheitsrelevante Störungen frühzeitig zu erkennen, korrekt zu bewerten und abgestimmte Gegenmaßnahmen einzuleiten, um Führungs- und Einsatzfähigkeit zu erhalten, mit dem Ziel, auch unter Angriff nicht zu einem „fail safe“, sondern zu einem kontrollierten „fight through“ fähig zu sein. Zweitens soll Cyber-Sicherheit fest in der militärischen Führung verankert werden. Cyber-Aspekte sind nicht als rein technische Querschnittsaufgabe zu verstehen, sondern als integraler Bestandteil der Planung, Vorbereitung und Durchführung militärischer Operationen. SOC und NOC werden in diesem Verständnis als wesentliche Elemente der Führungsunterstützung positioniert, die kontinuierlich Informationen zur Cyber-Lage bereitstellen und damit Entscheidungsprozesse auf allen Führungsebenen unterstützen. Drittens zielt das Ausbildungsprogramm auf den Aufbau eines gemeinsamen Lage- und Rollenverständnisses ab. Es schafft ein einheitliches Verständnis von Rollen, Prozessen und Schnittstellen zwischen SOC, NOC, Stäben, Führungsunterstützung, Spezialistinnen und Spezialisten für industrielle Steuerungs- und OT-Systeme sowie weiteren nationalen und gegebenenfalls multinationalen Partnern. Dadurch wird eine gemeinsame Sprache gefördert, die Zusammenarbeit im Rahmen von Übungen und Einsätzen erleichtert und die Grundlage für ein kohärentes, abgestimmtes Vorgehen im Cyber- und Informationsraum gelegt.

5.3.2 Zielsetzung des Curriculums

Das Curriculum verfolgt eine Reihe konkreter Ziele, die in den folgenden Kapiteln durch definierte Lernziele, klar strukturierte Module und abgestufte Qualifikationsstufen weiter operationalisiert werden. Im Kern geht es darum, die Fähigkeiten und das Verständnis der Angehörigen der Streitkräfte im Cyber- und Informationsraum systematisch zu entwickeln und so einen messbaren Beitrag zur Einsatz- und Führungsfähigkeit zu leisten.

Ein zentraler Zielbereich ist die Steigerung der Cyber-Awareness in den Streitkräften. Das Programm zielt darauf ab, ein gemeinsames Grundverständnis von Cyberbedrohungen, typischen Angriffsvektoren und den daraus resultierenden Risiken für militärische Operationen zu vermitteln. Die Teilnehmenden sollen erkennen, wie eng digitale Verwundbarkeiten mit der realen Operationsführung verknüpft sind und welche Rolle Informations- und Kommunikationstechnik für Planung, Führung und Wirkung haben. Besondere Aufmerksamkeit gilt dabei der Rolle des Menschen als kritischem Faktor: Von der persönlichen Cyber-Hygiene über den Umgang mit dienstlichen und privaten Endgeräten bis hin zur sicheren Nutzung von IT-Systemen und Kommunikationsmitteln im Einsatzgebiet werden Verhaltensweisen geschult, die das Risiko ungewollter Informationsabflüsse und erfolgreicher Angriffe deutlich reduzieren. Darauf aufbauend widmet sich ein weiterer Zielbereich dem Aufbau und der Vertiefung fachlicher Kompetenzen für SOC- und NOC-Personal. Die Teilnehmenden sollen fundierte Kenntnisse in den Bereichen System- und Netzwerksicherheit, Logdatenanalyse, Nutzung von SIEM-Technologien, Erkennung von Sicherheitsvorfällen (Incident Detection), strukturierte Reaktion auf solche Vorfälle (Incident Response) sowie grundlegende und fortgeschrittene forensische Fähigkeiten erwerben. Das Curriculum ist so gestaltet, dass Fachpersonal entlang klar definierter Qualifikationsstufen vom grundlegenden Operator über fortgeschrittene Analystinnen und Analysten bis hin zu Expertinnen und Experten für tiefgehende Analyse, Forensik, Threat Hunting und komplexen Netzwerkbetrieb entwickelt werden kann. Auf diese Weise wird ein professionelles Kompetenzprofil geschaffen, das den Anforderungen eines modernen militärischen SOC und NOC gerecht wird.

Ein weiterer Schwerpunkt liegt auf der Verbesserung der Reaktionsfähigkeit und Resilienz. Ziel ist es, die Zeitspanne zwischen dem Auftreten eines sicherheitsrelevanten Ereignisses, seiner Entdeckung und der Einleitung geeigneter Gegenmaßnahmen signifikant zu verkürzen. Die Teilnehmenden sollen in die Lage versetzt werden, Vorfälle nicht nur zu registrieren, sondern diese in ihrer operativen Relevanz zu bewerten, zu priorisieren und abgestimmt zu bearbeiten. Gleichzeitig sollen sie befähigt werden, auch unter laufenden Cyberangriffen den Betrieb kritischer Systeme aufrechtzuerhalten und, wo erforderlich, kontrolliert zu degradieren, anstatt funktionsunfähig zu werden. Damit wird das Prinzip der Resilienz – das „Durchhalten unter Angriff“ – praktisch mit Leben gefüllt. Ein weiterer Zielbereich ist die Stärkung von Kooperation, Interoperabilität und Führungsfähigkeit. Das Curriculum unterstützt die Verbesserung der Zusammenarbeit zwischen SOC, NOC, Stäben, nationalen Cyber-Kommandos sowie gegebenenfalls Bündnispartnern, indem es ein gemeinsames Vokabular, einheitliche Prozesse und abgestimmte Meldewege vermittelt. Die Teilnehmenden sollen befähigt werden, die Cyber-Lage adressatengerecht aufzubereiten – etwa für Kommandeure, Stäbe oder übergeordnete Dienststellen – und die gewonnenen Erkenntnisse strukturiert in militärische Entscheidungsprozesse einzubringen. Dadurch wird Cyber-Sicherheit nicht isoliert betrachtet, sondern als integraler Bestandteil der Führungs- und Operationsplanung verankert.

Schließlich zielt das Curriculum auf die Integration organisatorischer, rechtlicher und ethischer Rahmenbedingungen ab. Die Teilnehmenden lernen die für das Handeln im Cyber- und Informationsraum relevanten rechtlichen Grundlagen, Regelungen und Weisungen kennen, einschließlich Geheimschutz, Datenschutz, militärischer Sicherheitsbestimmungen und Rules of Engagement. Gleichzeitig wird ein Bewusstsein für ethische Fragestellungen und Verantwortlichkeiten im Umgang mit Daten, Analyse- und Angriffsmethoden sowie der beabsichtigten und unbeabsichtigten Wirkung im Cyber-Raum geschaffen. Damit trägt das Ausbildungsprogramm dazu bei, nicht nur fachlich versierte, sondern auch rechtlich und ethisch reflektierte Fachkräfte für SOC und NOC in den Streitkräften hervorzubringen.

5.3.3 Einordnung in strategische Rahmenbedingungen

Das Ausbildungsprogramm ist so konzipiert, dass es sich nahtlos in bestehende nationale und bündnisbezogene Cyber- und Verteidigungsstrategien einfügen lässt. Es versteht sich nicht als isolierte Maßnahme, sondern als konkreter Baustein zur operativen Umsetzung übergeordneter strategischer Vorgaben im Cyber- und Informationsraum. Durch seine modulare Struktur und die Ausrichtung an klar definierten Qualifikationsstufen kann das Curriculum an nationale Rahmenbedingungen, bestehende Doktrinen sowie an Anforderungen von Bündnissen und Koalitionen angepasst und in diese eingebettet werden.

Im Zentrum steht dabei die Ausprägung und Weiterentwicklung von Fähigkeiten im Cyber- und Informationsraum. Das Programm unterstützt den Aufbau von Kompetenzen, die für die Planung, Durchführung und Unterstützung militärischer Operationen in einer zunehmend digitalisierten und vernetzten Umgebung erforderlich sind. Gleichzeitig trägt es zur Stärkung der Resilienz kritischer militärischer Infrastrukturen bei, indem es das Personal befähigt, Verwundbarkeiten zu erkennen, Risiken realistisch zu bewerten und angemessene Schutz- und Reaktionsmaßnahmen zu planen und umzusetzen. Ein weiterer Schwerpunkt liegt auf der Vorbereitung der Streitkräfte auf hybride Bedrohungen und vernetzte Operationsformen, in denen klassische kinetische Wirkung, Informationsoperationen und Cyberangriffe miteinander verzahnt eingesetzt werden. Damit bildet das Curriculum die Grundlage für eine systematische und nachhaltige Qualifizierung von SOC- und NOC-Personal und leistet einen Beitrag dazu, Cyber-Sicherheit als festen Bestandteil militärischer Professionalität zu etablieren. Es unterstützt die Entwicklung eines gemeinsamen Verständnisses von Rollen, Verantwortlichkeiten und Prozessen im Cyber- und Informationsraum und trägt dazu bei, dass Cyber-Aspekte in Planung, Führung und Einsatzdurchführung nicht mehr als nachgeordnete Spezialthemen, sondern als integraler Bestandteil moderner Streitkräfte wahrgenommen und gelebt werden.

5.4 Ausbildungsziele

Die Ausbildungsziele operationalisieren die in Kapitel 5.3 formulierte Mission in überprüfbare Wirkungskategorien. Im Mittelpunkt steht nicht die erneute Beschreibung des Gesamtcurriculums, sondern die Übersetzung der Leitidee in konkrete Zielzustände für Wissen, Fähigkeiten, Verhalten und organisationsbezogene Wirksamkeit. Die nachfolgenden fünf Zielbereiche strukturieren daher den erwarteten Beitrag des Curriculums zur Einsatz- und Führungsfähigkeit im Cyber- und Informationsraum und bilden die Grundlage für Modulgestaltung, Qualifikationsstufen und Evaluation des Lernerfolgs (siehe Abbildung 28).

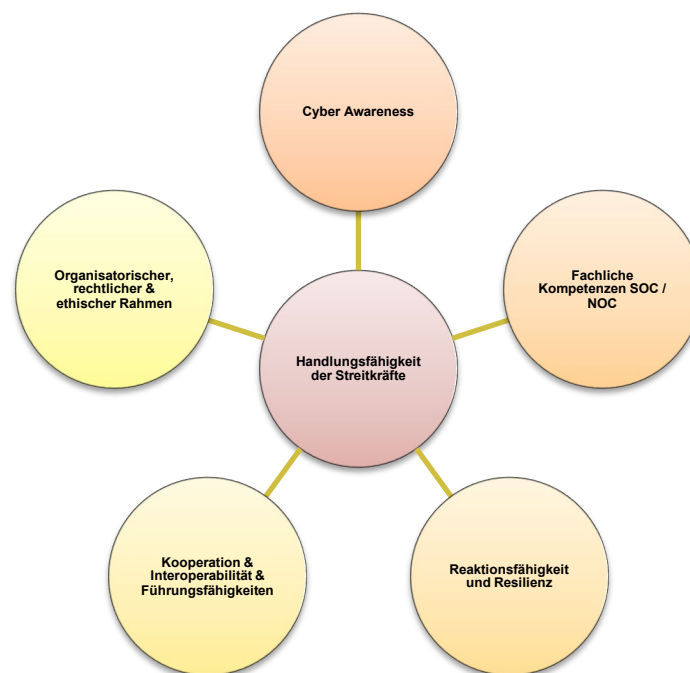


ABBILDUNG 28 ZUSAMMENSPIEL DER AUSBILDUNGSZIELE

5.4.1 Zielbereich 1: Steigerung der Cyber-Awareness in den Streitkräften

Ein zentrales Ausbildungsziel besteht in der nachhaltigen Steigerung der Cyber-Awareness in den Streitkräften. Die Teilnehmenden sollen ein gemeinsames Grundverständnis von Cyberbedrohungen, typischen Angriffsvektoren und den daraus resultierenden Risiken für militärische Operationen entwickeln. Sie erkennen, dass Schwachstellen in Informations- und Kommunikationssystemen direkte Auswirkungen auf Führungs- und Einsatzfähigkeit haben können und dass der Faktor Mensch dabei eine zentrale Rolle spielt. Cyber-Awareness wird dabei nicht als einmalige Sensibilisierung verstanden, sondern als kontinuierlicher Lern- und Reflexionsprozess, der die tägliche Praxis im Grundbetrieb wie im Einsatz nachhaltig prägt.

Konkret bedeutet dies, dass die Angehörigen der Zielgruppen grundlegende Konzepte wie Vertraulichkeit, Integrität und Verfügbarkeit, verschiedene Angriffsformen (z. B. Phishing, Ransomware, APT-Kampagnen) sowie die Besonderheiten hybrider Bedrohungen verstehen und auf ihre eigene Tätigkeit beziehen können. Sie sollen in der Lage sein, typische Indikatoren für Angriffe oder Fehlverhalten im eigenen Arbeitsumfeld zu erkennen und deren mögliche Auswirkungen auf die jeweilige Einheit, den Verband oder den gesamten Einsatz abzuschätzen. Gleichzeitig werden sie für Risiken sensibilisiert, die aus unbedachten Handlungen resultieren – etwa dem Umgang mit Passwörtern, mobilen Endgeräten, Wechseldatenträgern oder der Nutzung sozialer Medien im dienstlichen und privaten Kontext. Dazu gehört auch das Bewusstsein, dass

bereits scheinbar kleine Verstöße gegen Sicherheitsvorgaben – etwa die Nutzung privater Cloud-Dienste, das Fotografieren von Einrichtungen oder das Teilen von Standortdaten – von gegnerischen Akteuren systematisch ausgewertet und gegen die Streitkräfte verwendet werden können (siehe Abbildung 2). Die Ausbildung verfolgt dabei einen ganzheitlichen Ansatz: Neben der reinen Wissensvermittlung werden Verhaltensänderungen angestrebt. Durch praxisnahe Beispiele, Rollenspiele, Simulationen (z. B. Phishing-Kampagnen) und die Einbindung von Erfahrungsberichten aus Übungen und realen Vorfällen sollen die Teilnehmenden erkennen, wie sich Cyberbedrohungen konkret auswirken und welche Rolle sie persönlich bei der Abwehr einnehmen. Cyber-Awareness ist somit nicht nur Aufgabe von Spezialistinnen und Spezialisten in SOC und NOC, sondern Bestandteil militärischer Professionalität auf allen Ebenen. Mittelfristig soll erreicht werden, dass ein definierter Anteil der Teilnehmenden (z. B. mindestens 80 % nach einem Jahr Programmlaufzeit) in standardisierten Awareness-Tests signifikant bessere Ergebnisse erzielt und dass sich dieses Bewusstsein auch in Übungen und im Alltagsbetrieb nachweisen lässt, etwa durch eine geringere Zahl von sicherheitsrelevanten Fehlverhalten. Ergänzend können Kennzahlen wie die Meldequote verdächtiger E-Mails, die Teilnahmequote an Awareness-Maßnahmen oder die Ergebnisse von Übungsauswertungen herangezogen werden. Auf diese Weise wird Cyber-Awareness zu einer messbaren Fähigkeit, deren Entwicklung über die Zeit verfolgt und gezielt weiterentwickelt werden kann.

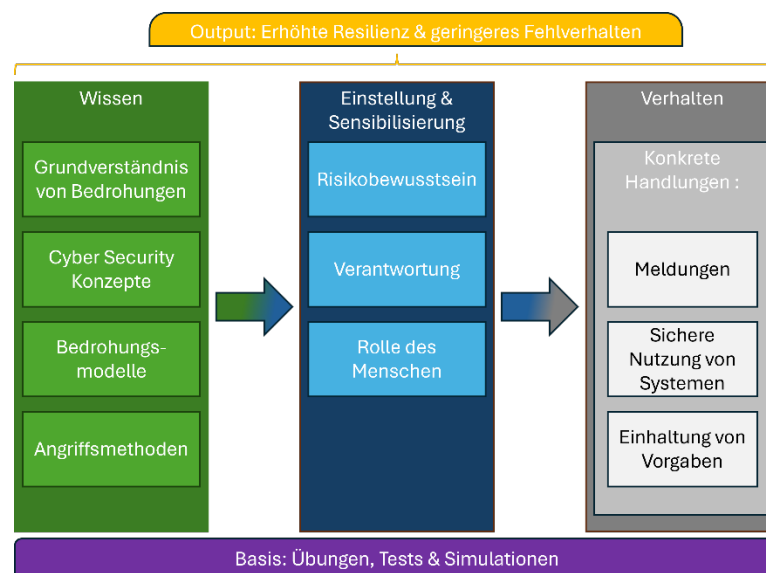


ABBILDUNG 29 ENTWICKLUNG VON CYBER-AWARENESS

5.4.2 Zielbereich 2: Aufbau und Vertiefung fachlicher Kompetenzen für SOC- und NOC-Personal

Ein weiterer zentraler Zielbereich des Curriculums ist der systematische Aufbau und die Vertiefung fachlicher Kompetenzen für das Personal in militärischen SOC und NOC. Das Ausbildungsprogramm verfolgt das Ziel, die Teilnehmenden schrittweise von einem grundlegenden Verständnis der eingesetzten Systeme und Netze hin zu einem professionellen Kompetenzniveau zu führen, das den Anforderungen eines modernen, operationellen Cyber- und Netzwerkbetriebs in den Streitkräften entspricht. Fachkompetenz wird dabei nicht nur als reine Beherrschung von Werkzeugen und Technologien verstanden, sondern als Kombination aus technischem Wissen, methodischem Vorgehen und der Fähigkeit, Entscheidungen unter Zeitdruck und im Verbund mit anderen Dienststellen zu treffen.

Dazu gehören fundierte Kenntnisse in System- und Netzwerksicherheit, der sichere Umgang mit Logdaten und Telemetrie, die Nutzung von SIEM- und Monitoring-Plattformen, die Erkennung und

Analyse von Sicherheitsvorfällen sowie die strukturierte Reaktion im Rahmen definierter Incident-Response-Prozesse. Die Teilnehmenden sollen in die Lage versetzt werden, Ereignisse nicht nur oberflächlich zu bearbeiten, sondern deren Ursachen zu verstehen, Zusammenhänge zu erkennen und Maßnahmen so zu wählen, dass sowohl technische als auch operative Auswirkungen berücksichtigt werden. Mit zunehmender Qualifikationsstufe kommen vertiefte Fähigkeiten hinzu, etwa im Bereich Threat Hunting, forensische Untersuchungen, Analyse komplexer Angriffskampagnen, die Korrelation unterschiedlicher Datenquellen oder die Planung und Optimierung von Sicherheitsarchitekturen für militärische Führungs- und Kommunikationssysteme. Ergänzend werden Fähigkeiten in der Erstellung von Lagebildern, Berichten und Entscheidungsvorlagen vermittelt, um die gewonnenen Erkenntnisse zielgerichtet in die militärische Führung einzuspeisen. Die Qualifikationsstufen sind so angelegt, dass das Personal entlang eines klar strukturierten Pfades vom Operator über die Analystin bzw. den Analysten bis hin zur Expertin bzw. zum Experten entwickelt werden kann. Jede Stufe baut inhaltlich auf der vorangegangenen auf und ist mit definierten Rollenbildern, typischen Aufgaben und erwarteten Verantwortlichkeiten verknüpft. Damit wird sichergestellt, dass die erworbenen Kompetenzen unmittelbar in der Praxis verortet sind – sei es in der Schicht im SOC, im Betriebskontext des NOC oder in der Funktion als fachliche Ansprechperson in Stäben und Führungsunterstützungseinrichtungen. Ein messbares Ziel kann beispielsweise darin bestehen, dass nach einem definierten Zeitraum ein bestimmter Anteil der in SOC und NOC eingesetzten Personen erfolgreich die jeweils nächsthöhere Qualifikationsstufe erreicht, die entsprechenden Leistungsnachweise erbringt und die erworbenen Fähigkeiten in Übungen und im Realbetrieb nachweislich anwendet. Dies kann über Prüfungen, Übungsauswertungen, Beurteilungen durch Vorgesetzte sowie über technisch-operative Kennzahlen im Betrieb überprüft werden.

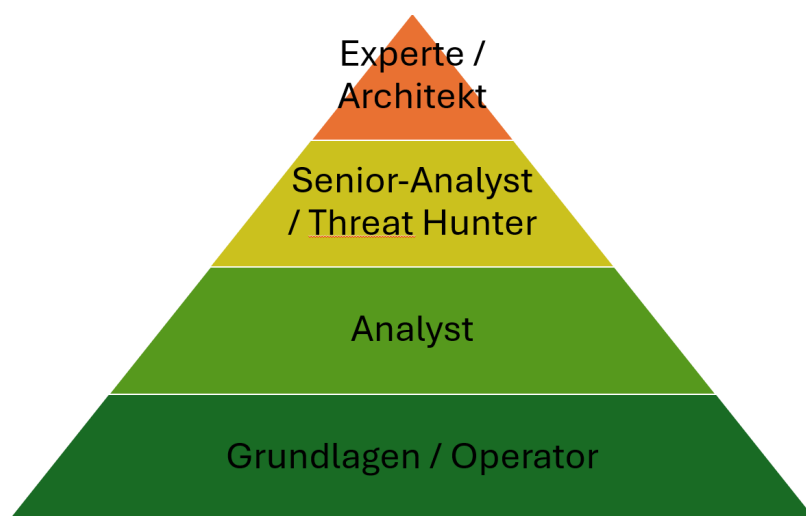


ABBILDUNG 30 STUFENMODELL DER FACHLICHEN KOMPETENZENTWICKLUNG IN SOC UND NOC

5.4.3 Zielbereich 3: Verbesserung der Reaktionsfähigkeit und Resilienz

Neben Wissen und Fertigkeiten zielt das Curriculum ausdrücklich auf eine spürbare Verbesserung der Reaktionsfähigkeit und Resilienz der Streitkräfte im Cyber- und Informationsraum ab. Im Mittelpunkt steht die Fähigkeit, sicherheitsrelevante Ereignisse frühzeitig zu erkennen, korrekt zu bewerten, Prioritäten zu setzen und geeignete Gegenmaßnahmen koordiniert einzuleiten. Reaktionsfähigkeit wird dabei nicht nur als technischer Prozess verstanden, sondern als Zusammenspiel aus klar definierten Abläufen, geübten Rollen, belastbaren Kommunikationswegen und einer gemeinsamen Lagewahrnehmung zwischen allen beteiligten Stellen.

Die Teilnehmenden sollen lernen, die Zeitspanne zwischen dem Auftreten eines Vorfalls, seiner Entdeckung und der Einleitung erster Maßnahmen deutlich zu verkürzen. Dazu gehört die sichere Nutzung von Alarmierungs- und Eskalationsprozessen, das strukturierte Abarbeiten von Playbooks sowie die enge Abstimmung zwischen SOC, NOC und weiteren beteiligten Stellen – etwa Stäben, Führungsunterstützung, Spezialistinnen und Spezialisten für OT oder externen Partnern. Sie sollen in der Lage sein, auch unter Zeitdruck und bei unvollständiger Informationslage handlungsfähig zu bleiben, Entscheidungen anhand definierter Kriterien zu priorisieren und diese nachvollziehbar zu dokumentieren. Gleichzeitig wird die Fähigkeit geschult, unter anhaltender Bedrohungslage den Betrieb kritischer Systeme aufrechtzuerhalten, alternative Kommunikationswege vorzubereiten und – wo erforderlich – Systeme kontrolliert zu degradieren, um einen vollständigen Ausfall zu vermeiden. Reaktion bedeutet in diesem Verständnis nicht nur „Feuer löschen“, sondern das bewusste Steuern von Degradation und Wiederherstellung im Sinne der militärischen Auftragserfüllung. Als messbare Ziele können etwa definiert werden, dass in Übungen mit realitätsnahen Angriffsszenarien die mittlere Zeit bis zur Erkennung eines Vorfalls (Mean Time to Detect, MTDD) und die mittlere Zeit bis zur Einleitung geeigneter Gegenmaßnahmen (Mean Time to Respond, MTTR) im Vergleich zu Ausgangswerten um einen festgelegten Prozentsatz reduziert werden. Ergänzend kann beurteilt werden, wie stabil die Aufrechterhaltung wesentlicher Dienste trotz Störungen gelingt – beispielsweise durch definierte Stresstests, Simulationen von Teilausfällen oder Szenarien mit überschneidenden Vorfällen. Auf dieser Grundlage lässt sich nachvollziehen, ob die im Curriculum vermittelten Inhalte tatsächlich zu einer erhöhten Resilienz beitragen und ob SOC- und NOC-Strukturen in der Lage sind, auch unter widrigen Bedingungen den Kernauftrag der Streitkräfte im Cyber- und Informationsraum zu unterstützen.



ABBILDUNG 31 REAKTIONSKETTE UND RESILIENZ IM CYBER- UND INFORMATIONSRAUM

5.4.4 Zielbereich 4: Stärkung von Kooperation, Interoperabilität und Führungsfähigkeit

Ein weiterer wichtiger Zielbereich des Curriculums ist die Stärkung von Kooperation, Interoperabilität und Führungsfähigkeit. Moderne Operationen im Cyber- und Informationsraum sind durch eine enge Verzahnung verschiedener militärischer und – je nach Lage – auch ziviler Akteure geprägt. Nationale Cyber-Kommandos, operative Stäbe, Führungsunterstützung, Nachrichtendienste, spezialisierte Fachstellen, internationale Hauptquartiere sowie gegebenenfalls Partnerbehörden und -organisationen arbeiten gemeinsam in einem hochdynamischen Informationsverbund. Das Curriculum trägt dieser Realität Rechnung, indem es gezielt darauf abzielt, ein gemeinsames Verständnis von Prozessen, Rollen und Schnittstellen zwischen SOC, NOC, Stäben, nationalen Cyber-Kommandos, Nachrichtendiensten, weiteren spezialisierten Dienststellen sowie Bündnis- und Koalitionspartnern zu entwickeln und zu festigen.

Im Mittelpunkt steht dabei die Einsicht, dass SOC und NOC zwar die technischen Schaltstellen für Erkennung, Analyse und Reaktion im Cyber- und Informationsraum sind, ihre Wirkung jedoch erst im Zusammenspiel mit den übrigen Akteuren voll zur Geltung kommt. SOC und NOC liefern kontinuierlich Daten, Bewertungen und technische Lageinformationen, die in Stäben und Führungsorganisationen zu einem übergreifenden Lagebild verdichtet werden. Dieses Lagebild fließt in operative und strategische Entscheidungsprozesse ein – etwa bei der Priorisierung von

Schutzmaßnahmen, der Anpassung von Einsatzplänen oder der Ressourcenallokation. Gleichzeitig erhalten SOC und NOC aus der Führungsebene Weisungen, Prioritäten und Rahmenbedingungen, innerhalb derer sie technische Maßnahmen planen und umsetzen. Das Curriculum macht diese Wechselwirkung explizit und vermittelt, wie Informationen aus SOC und NOC so aufbereitet werden, dass sie auf unterschiedlichen Führungsebenen wirksam genutzt werden können. Die Teilnehmenden sollen in die Lage versetzt werden, ihre eigene Rolle in diesem Gefüge klar zu erkennen und zu verstehen, wie ihre Arbeit in die Gesamtführung eingebettet ist. Dazu gehört das Wissen, welche Informationen in welcher Form an wen zu melden sind, wie technische Befunde in militärische Wirkzusammenhänge übersetzt werden und wie Rückmeldungen und Weisungen aus der Führung wieder in konkrete technische Maßnahmen überführt werden. Ein besonderer Schwerpunkt liegt auf der Fähigkeit, technische Sachverhalte adressatengerecht aufzubereiten – etwa in Form von Lagemeldungen, Lagebildern oder Kurzvorträgen für Kommandeure und Stäbe – und daraus abgeleitete Handlungsoptionen verständlich zu kommunizieren. Die Teilnehmenden sollen lernen, Risiken, Unsicherheiten und Annahmen transparent darzustellen, Alternativen und ihre jeweiligen Vor- und Nachteile zu benennen und damit fundierte Entscheidungen im Sinne des militärischen Auftrags zu unterstützen.

Kooperation und Interoperabilität werden dabei nicht nur innerhalb der eigenen Organisation betrachtet, sondern auch im Kontext von ressortübergreifender Zusammenarbeit und Bündnisverpflichtungen. Das Curriculum adressiert daher auch die Zusammenarbeit mit nationalen Cyber-Kommandos und Nachrichtendiensten sowie, wo relevant, mit Bündnis- und Koalitionspartnern. Die Teilnehmenden sollen mit grundlegenden Prinzipien standardisierter Meldewege, gemeinsamer Lageformate und abgestimmter Verfahren vertraut sein und verstehen, wie konsistente Lagebilder über mehrere Organisationen und Ebenen hinweg entstehen. Dazu gehört auch der sichere Umgang mit Einstufungen, Freigaben und Austauschregeln für sensible Informationen. Messbare Ziele können in diesem Zielbereich beispielsweise die Etablierung standardisierter Meldewege und Berichtsformate, die erfolgreiche Durchführung gemeinsamer Übungen mit klar definierten Kommunikations- und Entscheidungsprozessen sowie die positive Bewertung der Zusammenarbeit und Informationsqualität durch übergeordnete Führungsstellen sein. Ergänzend können Kennzahlen wie Vollständigkeit und Pünktlichkeit von Meldungen, die Konsistenz von Cyber-Lagebildern zwischen verschiedenen Ebenen oder die Anzahl und Qualität gemeinsamer, organisations- oder nationenübergreifender Lagebesprechungen herangezogen werden. Auf dieser Basis lässt sich nachvollziehen, ob das Curriculum tatsächlich zu einer verbesserten Kooperation, einer höheren Interoperabilität und einer gestärkten Führungsfähigkeit im Cyber- und Informationsraum beiträgt.

5.4.5 Zielbereich 5: Integration organisatorischer, rechtlicher und ethischer Rahmenbedingungen

Schließlich verfolgt das Curriculum das Ziel, organisatorische, rechtliche und ethische Rahmenbedingungen fest im Handeln von SOC- und NOC-Personal zu verankern. Cyber-Operationen und Verteidigungsmaßnahmen bewegen sich stets in einem Gefüge aus nationalem Recht, Völkerrecht, militärischen Vorschriften, Geheimschutzbestimmungen und konkreten Rules of Engagement. Entscheidungen im Cyber- und Informationsraum haben nicht nur technische, sondern oftmals auch politische, strategische und gesellschaftliche Implikationen. Gleichzeitig werfen sie ethische Fragen auf – etwa im Umgang mit großen Datenmengen, bei der Nutzung bestimmter Analyse- oder Eingriffsmethoden oder hinsichtlich der möglichen Auswirkungen auf unbeteiligte Dritte, verbündete Kräfte oder zivile Infrastrukturen. Das Curriculum trägt dem Rechnung, indem es rechtliche und ethische Aspekte nicht als Randthema oder „Anhang“ behandelt, sondern als integralen Bestandteil professionellen Handelns im SOC und im NOC.

Die Teilnehmenden sollen die für ihr Handeln relevanten rechtlichen Grundlagen, Regelungen und Weisungen kennen, sie auf typische Szenarien anwenden können und sich der persönlichen Verantwortung bewusst sein, die mit Entscheidungen und Maßnahmen im Cyber- und Informationsraum verbunden ist. Dazu gehört ein Verständnis für die Abgrenzung zwischen zulässiger Verteidigung, nachrichtendienstlicher Tätigkeit, aktiven technischen Gegenmaßnahmen und gegebenenfalls offensiven Cyber-Operationen sowie für die jeweils einschlägigen Genehmigungs- und Meldewege. Sie sollen wissen, wann Maßnahmen melde- oder genehmigungspflichtig sind, welche Stellen – etwa Rechtsberater, übergeordnete Kommandobehörden oder internationale Partner – einzubinden sind und wie der Grundsatz der Verhältnismäßigkeit praktisch umzusetzen ist. Ebenso wesentlich ist das Bewusstsein für Geheimschutz, Einstufung und Weitergabe sensibler Informationen: Wer darf was wissen, in welcher Form dürfen Daten verarbeitet, korreliert und gespeichert werden, und wo liegen die Grenzen zulässiger Analyse?

Organisatorisch betrachtet werden SOC und NOC im Curriculum als Teile eines umfassenden Sicherheits- und Führungsgefüges verstanden. Das Ausbildungsprogramm vermittelt daher auch Kenntnisse über Zuständigkeiten und Rollen – etwa von Informationssicherheitsbeauftragten, Datenschutzbeauftragten, Rechtsberatern, Aufsichts- und Kontrollgremien oder nationalen Cyber-Kommandos – und über die Einbindung dieser Stellen in den täglichen Betrieb und in besondere Lagen. Die Teilnehmenden sollen nachvollziehen können, wie interne Richtlinien, Weisungen und Standardarbeitsanweisungen (SOPs) entstehen, wie diese auf übergeordnete Strategien und Doktrinen zurückgehen und welche Pflichten sich daraus für die eigene Tätigkeit im Schichtdienst, in Übungen und im Einsatz ableiten. Organisatorische Klarheit wird dabei als Voraussetzung für rechtssicheres und verantwortungsvolles Handeln vermittelt. Ethische Aspekte ergänzen diesen Rahmen. Die Teilnehmenden sollen sich mit Fragen auseinandersetzen, die über die rein rechtliche Zulässigkeit hinausgehen: Welche Wirkung hat eine Maßnahme auf Vertrauen in digitale Systeme, auf die Zivilbevölkerung oder auf Partnerorganisationen? Welche Risiken entstehen, wenn aus technischer Sicht mögliche Schritte politisch oder gesellschaftlich unerwünscht sind? Wie wird verhindert, dass Verhaltensweisen Einzug halten, die zwar kurzfristig operationalen Nutzen versprechen, langfristig aber Normen, Werte und Glaubwürdigkeit der Streitkräfte untergraben? Das Curriculum fördert eine reflektierte Haltung, in der professionelle Verantwortung, Loyalität gegenüber Auftrag und Rechtsstaat sowie der Schutz von Menschen und Infrastrukturen zusammen gedacht werden. Dies schließt auch die Fähigkeit ein, Bedenken zu artikulieren, auf mögliche Grenzüberschreitungen hinzuweisen und in Zweifelsfällen aktiv fachlichen oder rechtlichen Rat einzuholen.

Didaktisch werden diese Inhalte nicht nur in Form von Vorträgen oder Überblicksdarstellungen vermittelt, sondern insbesondere über Fallstudien, Planspiele und Entscheidungsübungen. Anhand realitätsnaher Szenarien – etwa der Korrelation großer Datenmengen, der Beobachtung verdächtiger Muster in befreundeten Netzen oder der Abwehr eines Angriffs mit unklarer Herkunft – sollen die Teilnehmenden rechtliche Vorgaben, organisatorische Abläufe und ethische Überlegungen konkret anwenden. Sie üben, ihre Entscheidungen zu begründen, Alternativen abzuwägen, Risiken transparent zu machen und die eigene Rolle im Gefüge von Weisungen, Verantwortung und Kontrolle zu reflektieren. Auf diese Weise werden rechtliche und ethische Anforderungen vom abstrakten Regelwerk zum praktischen Handlungsrahmen im Alltag von SOC und NOC. Messbar wird dieser Zielbereich unter anderem durch die Bewertung rechtlich-ethischer Fallstudien, in denen die Teilnehmenden Entscheidungen nachvollziehbar begründen und deren Konsequenzen aufzeigen müssen. Hinzu kommt die korrekte Anwendung von Vorgaben in Übungen – etwa bei der Einstufung und Weitergabe von Informationen, bei der Einbindung von Rechtsberatern oder bei der Einhaltung von Meldekettens. Rückmeldungen von Rechtsberatern, Kommandeuren und Aufsichtsgremien zur Qualität der Entscheidungsfindung, zur Einhaltung von Vorgaben und zum Verantwortungsbewusstsein des Personals liefern zusätzliche Indikatoren



dafür, ob rechtliche und ethische Rahmenbedingungen im Alltag des SOC- und NOC-Betriebs tatsächlich verinnerlicht sind und gelebt werden. Ergänzend können auditierte Verfahren, die Anzahl und Schwere dokumentierter Verstöße gegen Vorgaben sowie die Ergebnisse interner und externer Überprüfungen herangezogen werden, um den Reifegrad in diesem Zielbereich kontinuierlich zu bewerten und das Curriculum bei Bedarf weiterzuentwickeln.

5.5 Didaktische Philosophie und Ansatz

Die didaktische Philosophie des Curriculums beschreibt, nach welchen lern- und ausbildungswissenschaftlichen Grundannahmen die Qualifizierung militärischen SOC- und NOC-Personals gestaltet wird. Sie begründet, warum das Curriculum auf Präsenz, Cyber-Lab (Range)-Nutzung, problemorientierte Szenarien, kollaborative Lagearbeit, reflektierte Praxis und normativ verantwortetes Handeln setzt. Damit schafft dieses Kapitel den interpretativen Rahmen für die nachfolgenden didaktischen Unteransätze und macht deutlich, dass die gewählte Ausbildungsgestaltung nicht zufällig, sondern systematisch aus den Anforderungen des Einsatzfeldes abgeleitet ist.

5.5.1 Grundgedanken der didaktischen Ausrichtung

militärisches SOC- und NOC-Personal in komplexen, hochdynamischen und sicherheitskritischen Umgebungen handlungsfähig sein muss. Diese Umgebungen sind geprägt durch eine hohe technische Komplexität, eine Vielzahl beteiligter Akteure, eine ständige Veränderung der Bedrohungslage sowie teilweise massive Konsequenzen für Auftragserfüllung, Sicherheit von Kräften und Schutz kritischer Infrastrukturen. In einem solchen Kontext ist reines Faktenwissen – das bloße Wiedergeben von Definitionen, Protokollen oder Tool-Funktionen – notwendig, aber bei weitem nicht hinreichend. Entscheidend ist vielmehr die Fähigkeit, Wissen in realitätsnahen Situationen anzuwenden, im Team zu agieren, unter Zeitdruck zu entscheiden und das eigene Handeln vor dem Hintergrund rechtlicher und ethischer Vorgaben zu reflektieren. Das Curriculum orientiert sich daher an einem Handlungskompetenzmodell, in dem fachliches Wissen, praktische Fertigkeiten und persönliche Haltungen zusammenwirken. Handlungskompetenz bedeutet hier, dass SOC- und NOC-Personal in der Lage ist, eine Lage fachlich korrekt einzuordnen, geeignete Optionen zu entwickeln, diese im Rahmen der militärischen und rechtlichen Vorgaben zu bewerten, Entscheidungen aktiv mitzugestalten und die Umsetzung der Maßnahmen im Team zu unterstützen.

Im Mittelpunkt steht damit nicht das bloße „Kennen“ von Konzepten, sondern die Entwicklung einer ganzheitlichen Handlungskompetenz, die drei Ebenen umfasst:

- Wissen (kognitive Ebene): Verständnis von Systemen, Netzen, Angriffsmethoden, Prozessen, Rollen und Rahmenbedingungen.
- Können (pragmatische Ebene): Fähigkeit, Werkzeuge zielgerichtet einzusetzen, Logs zu interpretieren, Playbooks abzuarbeiten, Maßnahmen anzustoßen und mit anderen Stellen zu kooperieren.
- Haltung (affektive Ebene): Verantwortungsbewusstsein, Sicherheits- und Risikobewusstsein, Bereitschaft zur Zusammenarbeit, Reflexionsfähigkeit sowie die Orientierung an rechtlichen und ethischen Vorgaben.

Das Curriculum geht dabei explizit davon aus, dass diese drei Ebenen nicht nacheinander, sondern miteinander verwoben entwickelt werden. Ein rein wissensorientierter Unterricht würde die Anforderungen des Einsatzfeldes verfehlen; ebenso wäre ein ausschließlich praxisorientiertes „Training-on-the-Job“ ohne theoretische Fundierung und Reflexion kurzsichtig. Die didaktische Ausrichtung sucht daher bewusst die Balance zwischen kognitiver Durchdringung, praktischer Anwendung und reflektierender Einordnung. Lernen wird in diesem Curriculum nicht als einmalige Wissensvermittlung verstanden, bei der Informationen von Lehrenden zu Lernenden „übertragen“ werden, sondern als fortlaufender Prozess, in dem Erfahrungen gesammelt, reflektiert, in Konzepte überführt und erneut in der Praxis erprobt werden. Dieser zyklische Lernbegriff orientiert sich an der Idee, dass Kompetenz schrittweise entsteht: durch Tun, Nachdenken über das Tun, Ableiten von Prinzipien und erneutes Handeln auf einer höheren Stufe. Für den militärischen Cyber-Kontext

ist dieser zyklische Charakter von Lernen besonders bedeutsam. Zum einen verändern sich Bedrohungslagen permanent: Neue Angriffsvektoren, Werkzeuge und Techniken treten auf, bekannte Methoden werden weiterentwickelt oder in neuen Kombinationen eingesetzt. Zum anderen werden Systeme und Architekturen kontinuierlich angepasst – etwa durch Modernisierung, Migration in neue Plattformen, Integration zusätzlicher Sensorik oder die Vernetzung mit Systemen von Partnern und Verbündeten. Hinzu kommt, dass Verfahren und Prozesse regelmäßig überarbeitet werden, etwa auf Basis von Lessons Learned aus Übungen, Einsätzen oder sicherheitsrelevanten Vorfällen.

Die Ausbildung soll vor diesem Hintergrund nicht nur den „Stand von heute“ abbilden, sondern vor allem die Fähigkeit fördern, sich in neuen Situationen zurechtzufinden, aus Erfolgen und Fehlern zu lernen und das eigene Handeln kontinuierlich zu verbessern. Dies bedeutet:

- Lernende sollen ermutigt werden, Hypothesen zu bilden, Annahmen zu prüfen und auf Basis neuer Informationen anzupassen, anstatt ausschließlich nach bekannten Mustern zu handeln.
- Fehler werden nicht als reine Misserfolge betrachtet, sondern als Lernanlässe, die systematisch ausgewertet werden: Was war die Ausgangslage? Welche Informationen lagen vor? Welche Annahmen wurden getroffen? Welche Alternativen wären möglich gewesen?
- Reflexion ist fester Bestandteil des Curriculums: Nach Übungen, insbesondere in der Cyber Range, werden Debriefings durchgeführt, in denen fachliche Aspekte, Entscheidungsprozesse, Teamdynamiken und die Einhaltung rechtlicher/ethischer Vorgaben gemeinsam analysiert werden.

Gerade im militärischen Umfeld, in dem Entscheidungen häufig unter Zeitdruck, bei unvollständiger Informationslage und mit hohen möglichen Auswirkungen getroffen werden müssen, ist diese Fähigkeit zur reflektierten Praxis zentral. Das Curriculum soll dazu beitragen, eine Kultur zu fördern, in der nicht nur schnelles Handeln, sondern auch begründetes und lernfähiges Handeln als Maßstab professioneller Qualität gilt.

Vor diesem Hintergrund kombiniert das Ausbildungsprogramm mehrere in der Bildungs- und Lehr-Lernforschung etablierte Ansätze und passt sie gezielt an den militärischen SOC-/NOC-Kontext an. Diese Ansätze sind:

- ein praxis- und erfahrungsorientierter Ansatz, der reale Arbeitskontexte und eine Cyber Range als zentrales Lerninstrument nutzt,
- eine problemorientierte und szenariobasierte Didaktik, die Lernen um konkrete Fälle und Lagen herum strukturiert,
- ein holistischer und interdisziplinärer Ansatz, der Technik, Organisation, Mensch, Recht und Ethik zusammen denkt,
- eine kollaborative, teamorientierte Ausrichtung, die der Realität gemeinsam arbeitender Schichten und Lagezentren entspricht,
- ein aktualitäts- und zukunftsorientierter Ansatz, der dynamische Entwicklungen im Cyber- und Informationsraum berücksichtigt,
- Elemente individueller Flexibilität und Selbststudium, die unterschiedliche Vorkenntnisse und Lernrhythmen aufgreifen,

- sowie eine ethik- und wertebasierte Philosophie, die rechtliche und moralische Verantwortung als Bestandteil professionellen Handelns versteht.

Alle Trainings finden bewusst vor Ort statt. Diese Entscheidung ist sowohl durch didaktische als auch durch organisatorische und sicherheitsrelevante Erwägungen motiviert. Präsenzformate ermöglichen die direkte Beobachtung und Steuerung von Lernprozessen, erleichtern die Arbeit an sensiblen oder klassifizierten Inhalten, fördern nonverbale Kommunikation und Teamkohäsion und erlauben die nahtlose Integration in bestehende militärische Übungsumgebungen. Insbesondere für die Arbeit in der Cyber Range, für Schichtsimulationen und Lagebesprechungen ist physische Präsenz der Beteiligten von großem Vorteil. Gleichzeitig werden begleitende Unterlagen als Offline-Material bereitgestellt, die der Vorbereitung, Vertiefung und Nachbereitung dienen. Diese Materialien – etwa Skripte, Reader, Checklisten, Fallstudien, Aufgaben und Zusammenfassungen – ermöglichen es den Teilnehmenden, sich vor Kursbeginn in zentrale Themen einzuarbeiten, während der Ausbildung Inhalte nachzuschlagen und nach Ende eines Moduls gezielt zu vertiefen. Auf diese Weise wird Präsenzlernen durch Selbststudium ergänzt, ohne von einer durchgehenden Online-Infrastruktur abhängig zu sein. Die Offline-Materialien dienen zudem als Referenz im späteren Dienstbetrieb und unterstützen so den Übergang von der Ausbildungs- zur Anwendungssituation. Die Kombination aus Präsenzformaten und Selbststudiumsanteilen unterstützt eine effiziente Nutzung der gemeinsamen Lernzeit. Grundlagen und wiederholbare Inhalte werden zum Teil in das individuelle Lernen verlagert; in der gemeinsamen Zeit liegt der Schwerpunkt auf interaktiven, problemorientierten und erfahrungsbasierten Lernformen wie Diskussionen, Übungen, Szenarien und Reflexion. Dadurch wird die begrenzte Ressource „gemeinsame Zeit in einem Raum“ dort eingesetzt, wo sie den größten Mehrwert generiert: bei Austausch, Kooperation, Feedback und praktischer Anwendung.

Das Curriculum nimmt darüber hinaus in den Blick, dass die Zielgruppen – je nach Herkunft, Verwendung und bisheriger Ausbildung – unterschiedliche Vorkenntnisse mitbringen. Einige verfügen über langjährige IT- oder Netzwerkerfahrung, andere kommen stärker aus Führungs-, Stabs- oder operativen Verwendungen. Die didaktische Philosophie trägt dem Rechnung, indem sie sowohl strukturierte Grundlagenangebote als auch Möglichkeiten zur Vertiefung vorsieht. Durch Selbststudiumsmaterialien, optionale Vertiefungseinheiten und unterschiedliche Anspruchsniveaus in Übungsaufgaben können Teilnehmende an unterschiedlichen Punkten anknüpfen, ohne dass der gemeinsame Kern des Curriculums verwässert wird. Ein weiterer zentraler Gedanke ist die Nachhaltigkeit des Lernens. Das Programm ist nicht als einmalige Qualifizierungsmaßnahme im Sinne eines „Abhakens“ konzipiert, sondern als Baustein in einer längerfristigen Kompetenzentwicklung. Die vermittelten Lernhaltungen – etwa die Bereitschaft zur fortlaufenden Weiterbildung, die systematische Nutzung von Lessons Learned oder die kritische Reflexion des eigenen Handelns – sollen die Teilnehmenden dazu befähigen, auch nach Abschluss formaler Ausbildungsabschnitte weiterzulernen. Berufliche Praxis, Übungen, Einsätze und neue technische Entwicklungen werden so zu kontinuierlichen Lernanlässen, die im Sinne der im Curriculum verankerten Philosophie genutzt und reflektiert werden können. Vor diesem Hintergrund wird deutlich, dass das Curriculum nicht nur Inhalte, sondern auch eine bestimmte Auffassung von Professionalität im militärischen Cyber-Kontext vermittelt: Professionalität bedeutet hier, fachlich kompetent, kooperationsfähig, reflektiert und verantwortungsbewusst zu handeln – unter den spezifischen Rahmenbedingungen von Einsatz, Auftrag und militärischer Organisation. Die didaktische Philosophie ist auf diese Zielsetzung ausgerichtet und bildet den Rahmen dafür, wie Inhalte ausgewählt, strukturiert und umgesetzt werden.

In den folgenden Unterkapiteln wird daher für jeden der genannten Ansätze – praxis- und erfahrungsorientierter Ansatz, problemorientierte und szenariobasierte Didaktik, holistischer und interdisziplinärer Ansatz, kollaborative, teamorientierte Ausrichtung, aktualitäts- und zukunftsorientierter Ansatz, Elemente individueller Flexibilität und Selbststudium sowie die ethik-

und wertebasierte Philosophie – im Detail erläutert, warum dieser Ansatz gewählt wurde, welchen Mehrwert er im militärischen SOC-/NOC-Kontext bietet, welche potenziellen Nachteile er mit sich bringen kann und wie diese durch die konkrete Gestaltung der Ausbildung adressiert werden. Auf diese Weise wird transparent, dass das Curriculum nicht zufällig gewachsen ist, sondern didaktisch begründet aufgebaut ist und sich konsistent an den Anforderungen des Einsatzfeldes orientiert.

5.5.2 Praxis- und erfahrungsorientierter Ansatz

Der praxis- und erfahrungsorientierte Ansatz geht davon aus, dass komplexe Fertigkeiten vor allem in authentischen Handlungssituationen entwickelt werden. Er knüpft an Theorien des Erfahrungslernens an, insbesondere an das Modell von David Kolb, das Lernen als zyklischen Prozess aus konkreter Erfahrung, reflektierender Beobachtung, abstrakter Begriffsbildung und erneuter aktiver Erprobung versteht. [102] Für das im Curriculum adressierte militärische SOC- und NOC-Personal bedeutet dies: Es reicht nicht, Angriffstypen, Protokolle oder Tools theoretisch zu kennen. Entscheidend ist die Erfahrung, in einer konkreten Lage Alarme zu bewerten, Hypothesen zu bilden, Maßnahmen einzuleiten, mit anderen Stellen zu koordinieren und die Folgen des eigenen Handelns unmittelbar zu erleben – und diese Erfahrungen anschließend systematisch zu reflektieren und zu verallgemeinern. Im Vordergrund steht damit das Prinzip „Lernen durch Tun“ in einer Umgebung, die den späteren Einsatzbedingungen möglichst nahekommt, ohne deren Risiken zu tragen. Die Ausbildung soll die Teilnehmenden schrittweise von geführten Übungen hin zu eigenständigem Handeln in komplexen, dynamischen Situationen führen. Dieses Verständnis spiegelt sich in der Gestaltung aller praktischen Elemente des Curriculums wider, insbesondere in der Nutzung einer Cyber Range.

Die Cyber Range bildet das zentrale Werkzeug des praxis- und erfahrungsorientierten Ansatzes. Unter einer Cyber Range wird eine Umgebung verstanden, in der reale oder realitätsnah emulierte IT-, OT- und Netzwerksysteme bereitgestellt werden, um Cyber-Szenarien in einem geschützten Rahmen durchzuspielen. [103], [104] Sie ermöglicht es, realitätsnahe Cyber-Szenarien in einer kontrollierten Umgebung nachzustellen: mehrstufige Angriffe, Seitwärtsbewegungen im Netz, Störungen in ICS-/OT-Teilsystemen, Ausfälle von Kommunikationswegen oder Fehlkonfigurationen mit operativer Wirkung. Die Teilnehmenden arbeiten mit realistischen Systemen und Werkzeugen, sehen die technischen Spuren im Monitoring, in Logs und Telemetriedaten und können Gegenmaßnahmen erproben. Aktuelle Studien zu Cyber-Range-Übungen zeigen, dass solche Umgebungen besonders geeignet sind, authentische Trainingssituationen zu schaffen, in denen Sicherheitspersonal „train as you fight“ – also so übt, wie es später auch arbeitet. [105] Die Teilnehmenden werden realistischen Angriffsszenarien und Störungen ausgesetzt, müssen im Team agieren, Informationen priorisieren, Entscheidungen treffen und diese im System umsetzen. Fehler werden hier ausdrücklich als Lernchance betrachtet, nicht als Versagen. Damit wird ein Lernklima gefördert, in dem das Ausprobieren von Strategien, das Testen von Hypothesen und das bewusste Reflektieren von Fehlentscheidungen möglich ist – ein Vorteil, den reale Einsatzumgebungen in dieser Form nicht bieten.

Der Mehrwert dieses Ansatzes liegt in der hohen Praxisnähe und der engen Kopplung an den späteren Dienst in Schicht- und Einsatzstrukturen. Neben fachlichen Fertigkeiten wie Loganalyse, Nutzung von SIEM- und Monitoring-Systemen, Incident Handling oder Forensik werden insbesondere Stressresistenz, Priorisierungsfähigkeit, Teamkoordination und Entscheidungsstärke trainiert. Cyber-Range-Übungen können so gestaltet werden, dass typische Belastungsfaktoren – Zeitdruck, Informationslücken, parallele Vorfälle, Kommunikationsstörungen – gezielt eingebaut werden, um die Handlungssicherheit der Teilnehmenden unter realistischen Rahmenbedingungen zu stärken. [106] Gleichzeitig wird das Prinzip „train as you fight“ konsequent umgesetzt: Rollen, Prozesse und Kommunikationswege werden so geübt, wie sie auch im realen SOC-/NOC-Betrieb vorgesehen sind. Die Teilnehmenden übernehmen im Wechsel verschiedene

Rollen (z. B. L1-Analyst, Incident Manager, NOC-Operator, Vertreter OT, Ansprechpartner für den Stab) und erfahren so, wie ihr eigenes Handeln in das Gesamtgefüge eingebettet ist. Dies unterstützt nicht nur die Entwicklung individueller Fähigkeiten, sondern auch das Verständnis für Schnittstellen, Abhängigkeiten und Verantwortlichkeiten zwischen unterschiedlichen Funktionsbereichen.

Der praxis- und erfahrungsorientierte Ansatz trägt darüber hinaus dazu bei, implizites Wissen aufzubauen – also jenes handlungsnah, schwer verbalisierbare „Bauchgefühl“, das erfahrene Analyst:innen und Operator:innen auszeichnet. Wiederholte Erfahrungen in ähnlichen, aber nicht identischen Lagen helfen dabei, Muster zu erkennen, Anomalien schneller zu bewerten und realistische Erwartungen an das Verhalten von Systemen und Angreifern zu entwickeln. Studien zu Cyber-Range-basierten Trainings berichten, dass Teilnehmende nach mehreren Übungen sicherer im Umgang mit Werkzeugen, souveräner in der Lagebeurteilung und reaktionsschneller in der Einleitung geeigneter Maßnahmen werden. [107]

Dem stehen jedoch auch Herausforderungen gegenüber, die in der Konzeption des Curriculums bewusst berücksichtigt werden. Praxisintensive Formate und Range-Übungen sind technisch und organisatorisch aufwendig: Sie erfordern eine geeignete Infrastruktur, ein belastbares Szenariokonzept, realistische, aber steuerbare Angriffs- und Störungsbilder sowie qualifizierte Instruktor:innen, die sowohl fachlich als auch didaktisch in der Lage sind, Übungen zu planen, durchzuführen und auszuwerten. In der Literatur wird zudem darauf hingewiesen, dass die Entwicklung von Cyber-Range-Szenarien fehleranfällig, ressourcenintensiv und ohne methodische Leitlinien schwer skalierbar sein kann. [103] [108] Hinzu kommt, dass für weniger erfahrene Teilnehmende die Gefahr der Überforderung besteht, wenn Szenarien zu komplex gestaltet sind oder zu viele neue Elemente gleichzeitig enthalten. Dies kann dazu führen, dass Lernende sich auf einfache „Trial-and-Error“-Strategien zurückziehen oder in reinen Tool-Bedienmustern hängen bleiben, ohne die zugrunde liegenden Konzepte zu verstehen. Neuere Arbeiten zu Cyber-Range-Übungen weisen explizit darauf hin, dass die Komplexität und Dichte von Übungen an das Vorwissen der Zielgruppe angepasst werden muss, um Überforderung zu vermeiden und nachhaltiges Lernen zu ermöglichen.

Das Curriculum begegnet diesen Herausforderungen durch mehrere Gestaltungsprinzipien:

1. **Stufenweise Steigerung der Komplexität.** Übungen in der Cyber Range sind entlang der Qualifikationsstufen strukturiert. Auf einfachen Niveaus arbeiten die Teilnehmenden mit klar umrissenen Szenarien, in denen nur wenige Variablen variieren und in denen Entscheidungswege noch stark geführt werden. Mit zunehmendem Level werden Szenarien komplexer, offener und weniger vorstrukturiert: mehrere gleichzeitige Vorfälle, unvollständige oder widersprüchliche Informationen, Abhängigkeiten zu OT-Systemen oder Interaktionen mit externen Akteuren. So wird eine didaktische Progression geschaffen, die Lernende fordert, aber nicht überfordert. [106]

3. **Klare Vor- und Nachbereitungsphasen.** Jede praxisintensive Übung wird eingerahmt durch strukturierte Briefings und Debriefings. In der Vorbereitung werden Zielsetzungen, Rollen, Rahmenbedingungen und Sicherheitsaspekte geklärt; wesentliche fachliche Grundlagen können über Offline-Unterlagen vorab erarbeitet werden. In der Nachbereitung werden technische Aspekte (Was ist passiert?), prozessuale Aspekte (Wie wurde reagiert?), kooperative Aspekte (Wie hat das Team funktioniert?) und rechtlich-ethische Aspekte (Welche Vorgaben waren relevant?) gemeinsam reflektiert. Damit wird der Erfahrungslernzyklus, Erfahrung, Reflexion, Konzeptualisierung, erneute Anwendung, bewusst geschlossen. [102]

4. **Wiederverwendbare und adaptierbare Szenariobausteine.** Um den Entwicklungsaufwand zu begrenzen und gleichzeitig Vielfalt zu ermöglichen, werden Szenarien in Bausteine zerlegt (z. B. bestimmter Angriffsvektor, bestimmtes OT-

System, spezifisches Kommunikationsproblem). Diese Bausteine können in unterschiedlichen Kombinationen eingesetzt und an die Zielgruppe angepasst werden. Forschungsarbeiten zu Cyber-Range-Design und Szenario-Engineering betonen den Nutzen solcher modularen Ansätze, um Standardisierung, Wiederverwendbarkeit und Qualitätssicherung zu unterstützen. [103], [108]

5. Aufgaben-, rollen- und entscheidungszentrierte Gestaltung. Um eine zu starke Fokussierung auf einzelne Tools zu vermeiden, wird jedes Szenario konsequent um Aufgaben, Rollen und Entscheidungslogiken herum gestaltet. Die Leitfrage lautet nicht: „Wie bediene ich Tool X?“, sondern: „Wie erkenne und bewerte ich diesen Vorfall, welche Optionen habe ich, wie koordiniere ich mich mit anderen und wie treffe ich eine nachvollziehbare Entscheidung?“ Werkzeuge werden als Hilfsmittel eingeführt, die unterschiedliche technische Aufgaben erfüllen können; sie sind austauschbar und werden bewusst variiert, um zu verdeutlichen, dass es auf Prinzipien und Prozesse ankommt, nicht auf die Beherrschung eines einzelnen Produkts.[105]
6. Verknüpfung mit anderen Lernformen. Der praxisorientierte Ansatz steht nicht isoliert, sondern ist eng mit anderen didaktischen Elementen des Curriculums verzahnt. Theoretische Inputs, Fallstudien, Diskussionen und Selbststudienphasen liefern das begriffliche und konzeptionelle Fundament, auf dem Range-Übungen aufbauen. Umgekehrt werden Erfahrungen aus der Praxis systematisch zurück in den Theorieunterricht gespiegelt. Diese Wechselseitigkeit trägt dazu bei, dass Erfahrungen nicht „unverdaut“ bleiben, sondern in übertragbare Einsichten überführt werden, die auch in neuen Situationen nutzbar sind.

Insgesamt unterstützt der praxis- und erfahrungsorientierte Ansatz – und insbesondere der gezielte Einsatz einer Cyber Range – das zentrale Ziel des Curriculums, operationale Handlungssicherheit im Cyber- und Informationsraum aufzubauen. Er macht abstrakte Inhalte greifbar, fördert individuelle und kollektive Lernprozesse und trägt zur Entwicklung jener Professionalität bei, die militärisches SOC- und NOC-Personal in modernen Konflikt- und Bedrohungsszenarien benötigt.

5.5.3 Problemorientierte und szenariobasierte Didaktik

Die problemorientierte und szenariobasierte Didaktik stellt konkrete Problem- und Lagesituationen in den Mittelpunkt des Lernprozesses. Sie knüpft an die Tradition des Problem-Based Learning (PBL) an, wie sie ursprünglich in der medizinischen Ausbildung entwickelt wurde und heute in vielen sicherheitskritischen Bereichen eingesetzt wird. Kerngedanke ist, dass Lernende nicht zuerst isoliert Inhalte „durchnehmen“, um sie später eventuell anzuwenden, sondern dass fachliche Inhalte von Beginn an eng mit relevanten Problemen verknüpft werden, die aus der beruflichen Praxis stammen oder ihr zumindest sehr nahekommen. [109] Für den Kontext militärischer SOCs und NOCs bedeutet dies, dass Lernende nicht abstrakt über Angriffsklassen, Normen oder Prozessmodelle sprechen, sondern an realitätsnahen Fällen arbeiten: ungewöhnliche Logmuster, verdächtige Netzwerkflüsse, Störungen in kritischen Führungs- oder Waffensystemen, Beeinträchtigungen von ICS-/OT-Komponenten oder hybride Bedrohungslagen, in denen Cyber-Ereignisse mit Desinformationskampagnen, physischen Sabotageakten oder elektronischer Kampfführung verknüpft sind. In solchen Szenarien analysieren die Teilnehmenden zunächst sichtbare Symptome (z. B. Alarime im SIEM, Peaks in der Netzwerkbelastung, Fehlermeldungen in ICS/HMI, Meldungen aus der Truppe), formulieren Hypothesen über mögliche Ursachen, definieren ihren Informationsbedarf, wählen geeignete Werkzeuge und Datenquellen aus und entwickeln schrittweise Handlungspläne. Sie müssen Entscheidungen darüber treffen, welche Indikatoren priorisiert werden, welche Systeme wie tief überprüft werden, wann eskaliert wird und welche Gegenmaßnahmen im Hinblick auf Auftrag, Resilienz und Verhältnismäßigkeit sinnvoll sind. Damit wird nicht nur vorhandenes fachliches Wissen aktiviert, sondern es entstehen

Diagnose- und Problemlösekompetenzen, wie sie im Alltag eines SOC-/NOC-Betriebs ständig benötigt werden: die Fähigkeit, aus unvollständigen Informationen auf wahrscheinliche Ursachen zu schließen, Hypothesen zu verwerfen oder zu bestätigen, Alternativen zu vergleichen und Entscheidungen zu begründen. Studien zum Problem-Based Learning zeigen, dass diese Lernform gerade solche Fertigkeiten fördert: flexible Wissensnutzung, systematisches Problemlösen, selbstgesteuertes Lernen und effektive Zusammenarbeit. Die Szenarien werden bewusst so gestaltet, dass sie typische Unschärfen und Unvollständigkeiten realer Lagen enthalten. Das bedeutet etwa:

- widersprüchliche Indikatoren aus unterschiedlichen Quellen,
- zeitliche Verzögerungen bei Meldungen oder Logbereitstellung,
- Informationslücken zu bestimmten Teilnetzen oder ICS-Segmenten,
- parallele Ereignisse, die zunächst nicht klar trennbar sind.

Dadurch üben die Teilnehmenden, mit Unsicherheit umzugehen, strukturiert nach zusätzlichen Informationen zu suchen und unter Zeitdruck Entscheidungen zu treffen, obwohl kein „perfektes“ Lagebild vorliegt – genau so, wie es im Einsatz- oder Schichtbetrieb typischerweise der Fall ist.

Der Mehrwert dieses Ansatzes besteht darin, dass die Relevanz der Inhalte unmittelbar erfahrbar wird: Die Teilnehmenden erleben direkt, warum bestimmte Konzepte (z. B. Log-Korrelation, Netzwerksegmentierung, Eskalations- und Meldewege, Playbooks, ROE) für die Lösung des Problems entscheidend sind. Fachbegriffe und Modelle werden nicht als abstrakte Theorie wahrgenommen, sondern als Werkzeuge, die helfen, ein konkretes Problem zu lösen. Das erhöht Motivation und Behaltensleistung nachweislich.[109] Zugleich fördert dieser Ansatz kritisches Denken, Kreativität und Priorisierungsfähigkeit. Lernende müssen abwägen, welche Hypothese plausibel ist, welche Daten wirklich benötigt werden und welche Schritte angesichts begrenzter Ressourcen (Zeit, Personal, Bandbreite) unmittelbar nötig sind und welche warten können. Szenariobasierte Ansätze in der Cybersecurity-Ausbildung zeigen, dass Lernende so näher an realen Kompetenzprofilen ausgebildet werden und weniger dazu neigen, rein „kochbuchartig“ Checklisten abzuarbeiten. [110], [111] Im militärischen Umfeld bietet die szenariobasierte Didaktik zudem die Chance, technische und operative Dimensionen enger zu verknüpfen. So können Szenarien entworfen werden, in denen ein technischer Vorfall konkrete Folgen für einen Übungs- oder Einsatzverband hat: z. B. der Ausfall einer Führungsverbindung während einer Operation, Beeinträchtigungen logistikrelevanter Systeme vor einem Verlegevorhaben oder eine ICS-Störung in einer kritischen Infrastruktur im Inland. Die Teilnehmenden sehen dadurch, dass Cyber-Lagen nicht isoliert, sondern in den Gesamtzusammenhang von Einsatzführung eingebettet sind.

Problemorientiertes und szenariobasiertes Lernen ist allerdings nicht frei von Herausforderungen. Offene, komplexe Problemstellungen können insbesondere Teilnehmende mit weniger Vorerfahrung überfordern oder frustrieren, wenn Struktur und Unterstützung fehlen. PBL-Forschung weist darauf hin, dass die Qualität von Lernprozessen stark von der Gestaltung der Probleme und von der Rolle der Lehrperson als Facilitator abhängt: Zu offene Probleme ohne Orientierung lassen Lernende „im Nebel stochern“; zu stark strukturierte Aufgaben dagegen reduzieren PBL auf reines Rätselraten mit verdeckter Musterlösung. [112] Auch der Zeitbedarf ist höher als bei klassischen Vortragsformaten: Szenarien müssen eingeführt, bearbeitet, diskutiert und reflektiert werden. Wenn diese Phasen nicht gut vorbereitet sind, besteht die Gefahr, dass zwar viel Aktivität, aber wenig gezieltes Lernen stattfindet. Studien betonen daher die Bedeutung von klaren Lernzielen, gut designten Szenarien und gezielten Reflexionsphasen zur Sicherung der Ergebnisse. [112]

Das Curriculum begegnet diesen Risiken mit mehreren didaktischen Maßnahmen:

1. Rahmung durch Leitfragen, Checklisten und Zwischenziele. Problemorientierte Phasen werden nicht als völlig offene „Sandbox“ gestaltet, sondern durch strukturierende Elemente gerahmt. Leitfragen helfen, die Analyse zu fokussieren („Was wissen wir sicher?“, „Was vermuten wir?“, „Welche Informationen fehlen?“). Checklisten unterstützen das systematische Vorgehen (z. B. bei der Incident-Analyse oder bei der Bewertung von Kritikalität). Zwischenziele machen klar, welche Zwischenstände erreicht sein sollen (z. B. vorläufige Hypothesen, priorisierte Maßnahmen, Entscheidungsvorlage für den Stab). So bleibt der Charakter eigenständigen Problemlösens erhalten, ohne die Lernenden alleine zu lassen.
2. Klarer Rollen- und Prozessbezug. Szenarien werden so gestaltet, dass sie typische Rollen und Prozesse im SOC-/NOC-Umfeld abbilden: Erstmeldung, erste Analyse durch L1, Eskalation an L2/L3, Einbindung des NOC, Abstimmung mit ICS-/OT-Verantwortlichen, Lageaufbereitung für den Stab, Dokumentation und Lessons Learned. Dadurch lernen Teilnehmende nicht nur Inhalte, sondern auch ihre Rolle im Gesamtprozess und die Zusammenarbeit mit anderen Akteuren.
3. Didaktische Progression der Szenarien. Die Szenarien folgen einer klaren Progressionslogik:
 - a. Auf niedrigeren Stufen eher stark geführte Fälle mit klarer Fragestellung, begrenztem Umfang und überschaubarer Komplexität.
 - b. Auf fortgeschrittenen Stufen zunehmend offene Szenarien, in denen mehrere parallele Ereignisse, hybride Bedrohungen oder unklare Verantwortungszuordnungen auftreten.
 - c. Auf Expertenlevel ggf. mehrtägige Lagen, in denen sich die Situation dynamisch weiterentwickelt und strategische Entscheidungen vorbereitet werden müssen.

Forschung zu PBL und scenario-based learning empfiehlt genau diese abgestufte Vorgehensweise, um eine Balance zwischen Herausforderung und Unterstützung zu schaffen.

1. Verzahnung mit Selbststudium und Input-Phasen. Grundlagenwissen – etwa zu bestimmten Angriffsklassen, Protokollen, Logging-Konzepten oder forensischen Methoden, wird nicht erst im Szenario „entdeckt“, sondern vorab durch kompakte Inputs und Selbststudienmaterialien vermittelt. In den Szenarien wird dieses Wissen angewendet, vertieft und in neue Kontexte übertragen. So entsteht ein Wechselspiel zwischen „Erarbeiten“ und „Erproben“, wie es auch in PBL-Modellen beschrieben wird: Theorie und Praxis stützen sich gegenseitig, statt getrennt nebeneinander zu stehen.[109]
2. Einbindung von Bewertung und Kompetenzmessung. Szenariobasierte Aufgaben eignen sich auch, um Kompetenzen differenziert zu bewerten – etwa durch beobachtete Verhaltensindikatoren, Szenario-Guiding-Questions oder strukturierte Bewertungsraster. In der Cybersecurity-Forschung gibt es bereits Ansätze, wie sich problemorientierte, szenariobasierte Lernformen zur Kompetenzmessung nutzen lassen. [110], [113] Das Curriculum greift diese Ideen auf, indem es z. B. die Qualität von Hypothesen, die Priorisierung von Maßnahmen oder die Klarheit von Lageberichten im Rahmen von Szenarien bewertet.

5.5.4 Holistischer und interdisziplinärer Ansatz

Der holistische und interdisziplinäre Ansatz dieses Curriculums betrachtet Cyber-Sicherheit ausdrücklich nicht als rein technisches Thema, sondern als Ergebnis des Zusammenspiels von Mensch, Technik und Organisation. Ausgangspunkt ist die Beobachtung, dass Sicherheitsvorfälle

nur selten auf eine einzelne technische Schwachstelle zurückzuführen sind. [114], [115] In der Praxis zeigt sich immer wieder, dass technische Lücken erst dann gravierende Wirkung entfalten, wenn sie auf mangelhafte Prozesse, unklare Zuständigkeiten, fehlende Sensibilisierung oder eine unzureichende Einbindung rechtlicher und politischer Rahmenbedingungen treffen. [116] Ein modernes militärisches SOC- und NOC-Ausbildungskonzept muss daher über die reine Vermittlung von Tools, Protokollen und Angriffsmustern hinausgehen und die Gesamtheit des sozio-technischen Systems in den Blick nehmen, in dem SOC und NOC agieren. Vor diesem Hintergrund verbindet das Curriculum technische Inhalte – etwa System- und Netzwerksicherheit, SIEM- und Monitoring-Konzepte, Incident Response, Forensik oder Threat Hunting – systematisch mit organisatorischen, rechtlichen und menschlichen Aspekten. [117] In den Lehrveranstaltungen und Übungen wird nicht bei der Frage stehengeblieben, wie ein bestimmtes Ereignis technisch zustande kommt oder wie ein bestimmtes Werkzeug zu bedienen ist. Es wird stets weitergefragt: Wie wird dieses Ereignis im militärischen Gefüge organisatorisch verarbeitet? Welche Meldekettengreifen, wer ist wofür verantwortlich, welche Eskalationsstufen sind vorgesehen? Wie ist die Situation rechtlich einzuordnen – etwa im Hinblick auf Geheimschutz, militärische Sicherheitsbestimmungen, Rules of Engagement oder internationales Recht? Und schließlich: Welche operative Bedeutung hat das Ereignis tatsächlich? Welche Auswirkungen sind auf den Auftrag, auf laufende Operationen, auf die Sicherheit von Kräften und auf kritische militärische und zivile Infrastrukturen zu erwarten? Um diese Fragen nicht abstrakt zu behandeln, werden in den Szenarien und Fallstudien die Rollen von Stäben, Führungsorganisationen, ICS-/OT-Verantwortlichen, nationalen Cyber-Kommandos, Nachrichtendiensten, Rechtsberatern und weiteren beteiligten Stellen explizit gemacht und aktiv einbezogen. [114] SOC- und NOC-Personal erlebt dadurch, dass es nicht isoliert in einem technischen „Nebenraum“ arbeitet, sondern Teil eines komplexen Verbundes ist, der von strategischer Ebene bis in den Schichtbetrieb hinein reicht. Entscheidungen im SOC und NOC werden so nicht nur als technische, sondern auch als organisatorische und operative Entscheidungen erkennbar, die Abhängigkeiten und Interessen verschiedener Akteure berücksichtigen müssen. Gleichzeitig lernen die Teilnehmenden, wie ihre technische Bewertung in Form von Lagebildern, Lagemeldungen oder Entscheidungsvorlagen in Stäben und Führungsstrukturen weiterverarbeitet wird und welche Anforderungen an Klarheit, Nachvollziehbarkeit und Verdichtung technischer Informationen gestellt werden.

Der Mehrwert dieses holistischen und interdisziplinären Ansatzes liegt in der Entwicklung eines Systemverständnisses, das für realistische Risikoabschätzungen, Priorisierungen und Entscheidungen unverzichtbar ist. [114] SOC- und NOC-Personal lernt, die Auswirkungen technischer Maßnahmen nicht nur auf einzelne Systeme oder Dienste, sondern auf den Gesamtauftrag mitzudenken: Was bedeutet es für die Lage, wenn zur Eindämmung eines Angriffs bestimmte Verbindungen abgeschaltet, ICS-Komponenten in einen sicheren Modus versetzt oder Kommunikationswege temporär umkonfiguriert werden? Welche Folgeeffekte sind zu erwarten, und welche Alternativen stehen zur Verfügung? Dadurch werden technische Empfehlungen so formuliert, dass sie für Führungsebenen anschlussfähig sind und in Entscheidungsprozesse integriert werden können. Gleichzeitig schärft der interdisziplinäre Blick das Bewusstsein dafür, dass nicht jede technisch mögliche Maßnahme operativ sinnvoll, rechtlich zulässig oder politisch gewünscht ist. Der Ansatz trägt auch dazu bei, die häufig zu beobachtende Trennung von „Technikern“ und „Führung“ zu überwinden. Durch die systematische Verzahnung von technischen und nichttechnischen Inhalten lernen SOC- und NOC-Angehörige, die Sprache der Führungsebenen besser zu verstehen [117] und technische Sachverhalte so zu übersetzen, dass Kommandeurinnen und Kommandeure, Stabsoffiziere oder Rechtsberater:innen sie in ihren eigenen Entscheidungslogiken verarbeiten können. Umgekehrt wird deutlich, welche Informationen Führungsebenen tatsächlich benötigen, um zwischen verschiedenen Cyber-Risiken, Maßnahmen und Nebenwirkungen abzuwägen. Der interdisziplinäre Charakter der Ausbildung wirkt damit auch als Brücke zwischen unterschiedlichen „Kulturen“ innerhalb der Streitkräfte:

zwischen IT- und OT-Fachpersonal, operativen Einheiten, Stäben, juristischer Expertise und strategischer Ebene.

Die Herausforderung dieses Ansatzes besteht darin, die Vielzahl von Perspektiven, Ebenen und Fachlogiken so zu integrieren, dass Teilnehmende nicht überfordert werden. Wer sich gerade in technische Grundlagen einarbeitet, kann schnell überlastet sein, wenn gleichzeitig rechtliche, organisatorische und operative Dimensionen in voller Tiefe adressiert werden. Um dies zu vermeiden, setzt das Curriculum auf einen gestuften Aufbau. Zunächst werden in klar abgegrenzten Modulen Kerninhalte pro Bereich vermittelt: technische Grundlagen in System- und Netzwerksicherheit, grundlegende Konzepte von Meldekettens und Rollen, elementare Prinzipien des militärischen Führungsprozesses sowie die wichtigsten rechtlichen und ethischen Rahmenbedingungen. Diese Inhalte werden bewusst in einer für die Zielgruppe verständlichen Tiefe behandelt, ohne sofort alle möglichen Spezialfälle abzudecken. In einem zweiten Schritt werden diese Bereiche in integrierten Szenarien und Fallstudien zusammengeführt. Ein technischer Vorfall wird dann nicht mehr nur aus Sicht der Logs und Pakete betrachtet, sondern gleichzeitig aus der Perspektive eines Stabslements, eines ICS-Betreibers, einer Rechtsberatung oder eines Führungsorgans. Die Teilnehmenden wechseln dabei teilweise auch die Rolle: Wer in einer Übung als Analyst oder Operator agiert, nimmt in einer anderen als Vertreter einer Stabsfunktion oder als ICS-Verantwortliche:r teil. Auf diese Weise entstehen Erfahrungen, die deutlich machen, welche Informationen jeweils benötigt werden, wo typische Missverständnisse entstehen und wie man diese gezielt vermeiden kann. Wiederkehrende Querverweise und Beispiele helfen, die Verknüpfungen zwischen den Disziplinen zu festigen, ohne die kognitive Belastung unnötig zu erhöhen. So werden etwa bei technischen Übungen Hinweise auf die relevanten Meldekettens und Rechtsgrundlagen gegeben; in rechtlich-ethischen Fallstudien wird auf die technischen Handlungsoptionen rekurriert; in Übungen zu Stabsprozessen wird explizit thematisiert, welche Informationen aus SOC und NOC dort wie einfließen. Schritt für Schritt entsteht so ein konsistentes Bild, in dem die einzelnen Elemente – Technik, Organisation, Mensch, Recht, Ethik, Operation – nicht mehr nebeneinanderstehen, sondern als Teile eines Gesamtgefüges wahrgenommen werden.

Auf diese Weise trägt der holistische und interdisziplinäre Ansatz dazu bei, dass SOC- und NOC-Personal nicht nur als technisch versierte Spezialistinnen und Spezialisten agiert, sondern als integrierter Teil der militärischen Führungs- und Einsatzfähigkeit. Sie verstehen, wie ihr Handeln dazu beiträgt, den Auftrag zu erfüllen, Kräfte zu schützen, kritische Infrastruktur zu sichern und rechtliche sowie ethische Vorgaben einzuhalten. Damit unterstützt dieser Ansatz unmittelbar das Ziel des Curriculums, Cyber-Sicherheit als festen Bestandteil militärischer Professionalität zu verankern – nicht nur in den Systemen, sondern im Denken und Handeln der Menschen, die sie betreiben.

5.5.5 Kollaborative, teamorientierte Ausrichtung

Die kollaborative, teamorientierte Ausrichtung des Curriculums trägt der Tatsache Rechnung, dass SOC- und NOC-Tätigkeiten inhärent teambasiert sind. Schichtbetrieb, Übergaben, parallele Bearbeitung von Incidents, gemeinsame Lagebesprechungen und die ständige Abstimmung mit anderen Einheiten machen deutlich, dass Einzelkötter ohne ausgeprägte Teamfähigkeit im operativen Alltag rasch an Grenzen stoßen. Forschung zu kooperativem Lernen und Teamarbeit zeigt seit Jahrzehnten, dass gut gestaltete Zusammenarbeit nicht nur fachliche Leistungen steigert, sondern auch Motivation, Verantwortungsübernahme und soziale Kompetenzen fördert. [118], [119] Diese Erkenntnisse werden im Curriculum bewusst aufgegriffen und auf den militärischen SOC-/NOC-Kontext übertragen. Konkret bedeutet dies, dass kollaborative Lernformen nicht als „Ergänzung“, sondern als zentrales didaktisches Element eingesetzt werden. In Gruppenarbeiten, Teamübungen in der Cyber Range, Rollenspielen und Lagebesprechungen übernehmen die

Teilnehmenden definierte Rollen, etwa als L1-Analyst, Incident Manager, NOC-Operator, Vertreterin bzw. Vertreter für ICS/OT, Stabsoffizier oder Rechtsberatung. Dadurch erleben sie unmittelbar, wie Informationen zwischen den Funktionen fließen müssen, welche Missverständnisse typischerweise auftreten, wie wichtig klare Sprache, strukturierte Übergaben und eine gemeinsame Lagewahrnehmung sind und wie Entscheidungen gemeinsam vorbereitet und kommuniziert werden. Szenarien sind so konzipiert, dass sie nicht nur technische Aufgaben enthalten, sondern auch Kommunikations- und Abstimmungsaufgaben: Wer informiert wen, in welcher Form, mit welchem Detaillierungsgrad, und welche Rückfragen sind zu erwarten? Besonders bedeutsam ist dabei der Fokus auf sogenannte nicht-technische Fähigkeiten (Non-Technical Skills, NTS), wie sie aus der Crew Resource Management- und Crisis Resource Management-Forschung in Luftfahrt, Medizin und anderen Hochrisikobereichen bekannt sind: Teamwork, Kommunikation, Führungsverhalten, Situationsbewusstsein und gegenseitige Unterstützung.[120], [121] Im Curriculum werden diese Fähigkeiten explizit adressiert, indem Teamübungen die Teilnehmenden dazu anregen, Rollen klar zu übernehmen, Prioritäten transparent zu machen, Rückmeldungen einzuholen und Kritik offen zu äußern. In Stresssituationen – etwa bei gleichzeitigen Incidents oder unklaren Lagen – üben die Lernenden, ruhig und strukturiert zu kommunizieren, Verantwortung zu teilen und dennoch klare Entscheidungen herbeizuführen.

Der Mehrwert dieses Ansatzes liegt in der parallelen Förderung fachlicher und sozialer Kompetenzen. Die Teilnehmenden entwickeln ein gemeinsames Vokabular, lernen zentrale Begriffe und Konzepte so zu nutzen, dass sie zwischen verschiedenen Funktionen (SOC, NOC, ICS/OT, Stab) verständlich bleiben, und können die Perspektiven anderer Rollen besser nachvollziehen. Untersuchungen zu teamorientierten Lernformaten und kooperativen Methoden zeigen, dass solche Settings das Verständnis für unterschiedliche Expertisen vertiefen, Vertrauen aufbauen und die Qualität gemeinsamer Entscheidungen erhöhen.[122], [123] Im militärischen SOC-/NOC-Kontext ist dieses Vertrauen eine wesentliche Grundlage für erfolgreiche Zusammenarbeit – insbesondere in Lagen, in denen schnelle Entscheidungen mit potenziell weitreichenden Folgen getroffen werden müssen. Ein weiterer Aspekt der kollaborativen Ausrichtung ist die gezielte Vorbereitung auf interdisziplinäre Zusammenarbeit in Sicherheits- und Incident-Response-Teams. Studien zu Teamarbeit in der Cybersecurity-Ausbildung und in Incident-Response-Trainings zeigen, dass reine Einzelaufgaben die Realität moderner Cyberooperationen kaum abbilden. Stattdessen sind Übungen dann besonders wirksam, wenn sie Teamkoordination, Rollenverständnis und Wissensaustausch explizit in den Vordergrund stellen. [124], [125] Das Curriculum greift diese Erkenntnisse auf, indem es Aufgaben so gestaltet, dass sie nur im Team lösbar sind und die Stärken der unterschiedlichen Rollen erfordern – etwa bei der Zusammenführung von Netzwerk-, System-, ICS- und Lageinformationen in einem gemeinsamen Lagebild oder bei der abgestimmten Vorbereitung einer Entscheidungsvorlage für die Führung. Gleichzeitig werden mögliche Nachteile kooperativer Lern- und Arbeitsformen ausdrücklich berücksichtigt. In der pädagogischen Forschung ist bekannt, dass Gruppenarbeit zu ungleicher Beteiligung führen kann: Einige Personen übernehmen viel Verantwortung, andere ziehen sich zurück („Trittbrettfahren“), wiederum andere dominieren Diskussionen und Entscheidungen. [118] Diese Dynamiken sind auch in technischen Teams, einschließlich SOC- und NOC-Umgebungen, beobachtbar und können die Leistungsfähigkeit der Gruppe erheblich beeinträchtigen, wenn sie nicht gezielt adressiert werden.

Das Curriculum begegnet diesen Risiken durch mehrere Gestaltungsprinzipien. Erstens werden in Übungen klare Rollenzuweisungen vorgenommen: Jede Person übernimmt eine definierte Funktion mit spezifischem Verantwortungsbereich. So wird transparent, wer welche Beiträge liefern soll, und es fällt leichter, ungleiche Beteiligung zu erkennen und anzusprechen. Zweitens wird mit bewusst klein gehaltenen Lerngruppen gearbeitet, in denen sich alle aktiv einbringen können und niemand „untertaucht“. Drittens werden individuelle Teilaufgaben innerhalb von Teamaufgaben

vorgesehen – etwa das eigenständige Erstellen eines Teilabschnitts eines Lageberichts oder die Vorbereitung einer bestimmten Analyse –, sodass sowohl Teamleistung als auch individuelle Beiträge erkennbar werden. Ein zentrales Element ist zudem die systematische Beobachtung und Auswertung von Gruppenphasen. Instruktor:innen nehmen nicht nur die fachlichen Ergebnisse in den Blick, sondern achten ausdrücklich auf Kommunikations- und Kooperationsverhalten: Wie werden Informationen geteilt? Werden Rückfragen gestellt? Wie wird mit Dissens umgegangen? Wer kommt zu Wort, wer nicht? Dieses Beobachtungswissen fließt in strukturierte Debriefings ein, in denen gemeinsam reflektiert wird, was gut funktioniert hat und wo Kooperation verbessert werden kann. Simulationen, Teamübungen in der Cyber Range und tabletop exercises werden so nicht nur zu Orten fachlichen Trainings, sondern auch zu Lerngelegenheiten für Team- und Kommunikationskompetenz. [121], [125] Darüber hinaus können bewusst gestaltete Teamaufgaben dazu genutzt werden, Führungs- und Followership-Kompetenzen zu entwickeln. In wechselnden Szenarien erhalten unterschiedliche Personen die Rolle der Einsatz- oder Incident-Leitung und müssen Entscheidungen moderieren, Prioritäten setzen, Delegation vornehmen und Rückmeldungen einholen. Studien zu Crew Resource Management und teamorientierten Trainings in sicherheitskritischen Bereichen zeigen, dass der Wechsel zwischen Führungs- und Unterstützerrollen wesentlich dazu beiträgt, Verständnis für beide Perspektiven zu entwickeln und starre Hierarchiebilder zugunsten flexibler, kompetenzorientierter Führung zu überwinden. [120] Dieses Prinzip wird im Curriculum gezielt aufgegriffen, um militärische Führungsgrundsätze mit modernen Vorstellungen von Teamarbeit im Cyber- und Informationsraum zu verbinden.

Insgesamt trägt die kollaborative, teamorientierte Ausrichtung des Curriculums dazu bei, dass SOC- und NOC-Personal nicht nur als fachlich versierte Einzelpersonen ausgebildet wird, sondern als Teil leistungsfähiger, resilienter Teams. Die Teilnehmenden lernen, Wissen zu teilen, Stärken zu kombinieren, Schwächen zu kompensieren, unter Belastung konstruktiv zu kommunizieren und gemeinsam Verantwortung für Entscheidungen zu übernehmen. Damit unterstützt der Ansatz unmittelbar das Ziel, im militärischen Cyber- und Informationsraum nicht nur technisch, sondern auch organisatorisch und menschlich leistungsfähige Strukturen aufzubauen.

5.5.6 Aktualitäts- und zukunftsorientierter Ansatz

Die Bedrohungslage im Cyber- und Informationsraum ist von einer hohen und weiter zunehmenden Dynamik geprägt. Neue Angriffsformen, Tools und Technologien entstehen in kurzen Zyklen, bestehende Werkzeuge werden laufend weiterentwickelt, und Bedrohungsakteure nutzen zunehmend Automatisierung, KI-gestützte Verfahren und hybride Methoden. Aktuelle Lageberichte, etwa der EU-Agentur ENISA, betonen, dass Entscheidungsträger, Sicherheitsverantwortliche und operative Kräfte auf aktuelle, belastbare Bedrohungsinformationen angewiesen sind, um Risiken angemessen einschätzen und Maßnahmen planen zu können. [126] Vor diesem Hintergrund wäre ein Curriculum, das einmal festgeschrieben und dann über Jahre unverändert bleibt, innerhalb kurzer Zeit teilweise veraltet und würde die Anforderungen an modernes SOC- und NOC-Personal nur unzureichend abdecken. Das vorliegende Programm ist deshalb bewusst aktualitäts- und zukunftsorientiert angelegt. Es trägt dem Spannungsfeld Rechnung, dass Cyber-Ausbildung einerseits auf stabilen Grundlagen basieren muss, andererseits aber flexibel genug sein muss, um neue Entwicklungen aufnehmen zu können. Forschungsarbeiten zur Gestaltung von Cybersecurity-Curricula weisen genau auf dieses Spannungsfeld hin: Ein Curriculum, das nur aktuelle Tools und „Mode-Themen“ sammelt, ist ebenso wenig tragfähig wie eines, das sich ausschließlich an zeitlosen Grundlagen orientiert und die sich wandelnde Bedrohungslandschaft ignoriert. [127], [128], [129], [130]

Kern der Konzeption ist daher ein stabiler Grundstock an Konzepten, ergänzt um flexible, regelmäßig aktualisierte Bausteine. Der stabile Kern umfasst grundlegende Inhalte wie Netzwerktopologien und -protokolle, Sicherheitsprinzipien (Vertraulichkeit, Integrität,

Verfügbarkeit, Authentizität), klassische Angriffskategorien, Basiskonzepte der System- und Netzwerksicherheit, grundlegende Logging- und Monitoring-Prinzipien sowie etablierte Vorgehensmodelle der Incident Response. Diese Grundlagen ändern sich zwar im Detail, aber deutlich langsamer als konkrete Angriffsvarianten oder einzelne Produkte. Sie bilden das „tragende Gerüst“, auf dem das gesamte Curriculum aufbaut. Ergänzend dazu existiert eine Schicht flexibler Bausteine, in der aktuelle Entwicklungen gezielt aufgegriffen werden. Dazu gehören:

- aktuelle Fallstudien realer Vorfälle, insbesondere aus dem militärischen, behördlichen oder kritischen-Infrastrukturbereich,
- regelmäßig angepasste Szenarien in der Cyber Range, die neue Angriffsformen, Tools oder Taktiken (z. B. neue Ransomware-Familien, Cloud-bezogene Angriffe, KI-unterstützte Phishing-Kampagnen) abbilden,
- aktualisierte Use Cases und Playbooks, die auf Basis von Lessons Learned aus Übungen, Einsätzen und realen Incident-Response-Fällen überarbeitet werden,
- zusätzliche Module oder Vertiefungseinheiten zu neuen Technologien, etwa bestimmten Cloud-Architekturen, Zero-Trust-Konzepten oder neuen OT-/ICS-Plattformen, sofern diese für die Zielorganisation relevant sind.

Erkenntnisse aus militärischen SOC- und NOC-Übungen, aus dem tatsächlichen Schicht- und Einsatzbetrieb, aus nationalen und multinationalen Kooperationen sowie aus der einschlägigen Forschung werden systematisch erfasst und in die Weiterentwicklung dieser flexiblen Bausteine eingespeist. Studien zur Cybersecurity-Bildung betonen genau diese Notwendigkeit, Curricula auf Basis von empirischen Erfahrungen und Forschungsergebnissen regelmäßig zu überprüfen und anzupassen, anstatt sie nur sporadisch oder ad hoc zu verändern. [127], [129], [130] Der Mehrwert dieses aktualitäts- und zukunftsorientierten Ansatzes zeigt sich auf mehreren Ebenen. Zum einen lernen die Teilnehmenden, sowohl auf zeitlose Prinzipien als auch auf aktuelle Entwicklungen zurückzugreifen. Sie erkennen, dass ein gutes Verständnis von Netzwerkkonzepten, Protokollen oder Sicherheitsprinzipien notwendig ist, um neue Angriffsmuster einordnen und neue Tools kompetent einsetzen zu können. Zum anderen erleben sie, dass Veränderung im Cyber-Bereich die Norm ist: Neue Bedrohungen, neue Technologien und neue organisatorische Anforderungen werden nicht als Ausnahme, sondern als Bestandteil des Berufsbildes vermittelt. Damit unterstützt das Curriculum die Entwicklung einer Haltung des lebenslangen Lernens. Literatur zu professioneller Entwicklung in der Cybersecurity weist immer wieder darauf hin, dass fachliche Kompetenz nur dann aufrechterhalten werden kann, wenn Fachkräfte kontinuierlich lernen, etwa im Rahmen von Fortbildungen, Konferenzen, Exercises, Zertifizierungen oder eigenem Selbststudium. [131] Indem das Curriculum aktuelle Entwicklungen systematisch integriert und entsprechende Erwartungshaltungen formuliert, signalisiert es, dass auch nach Abschluss der formalen Ausbildung eine fortlaufende Aktualisierung von Wissen und Fähigkeiten Teil des professionellen Selbstverständnisses von SOC- und NOC-Personal ist. Gleichzeitig wird der Risikoaspekt eines starken Aktualitätsbezugs ausdrücklich reflektiert. Eine zu starke Fokussierung auf aktuelle „Mode-Themen“ – etwa einzelne Tools, spezifische Malware-Familien oder kurzfristig prominente Bedrohungstypen – birgt die Gefahr, dass grundlegende Konzepte vernachlässigt werden. Forschung zur Curriculumentwicklung in der Cybersecurity kritisiert genau solche Tendenzen und empfiehlt ausdrücklich, zwischen einem stabilen Konzeptkern und einer flexiblen Aktualisierungsschicht zu unterscheiden. [127], [128], [129]

Dem begegnet das Curriculum durch eine klare inhaltliche und strukturelle Trennung von Grundlagemodulen und Aktualisierungsbausteinen. Die Grundlagemodule definieren ein Mindestmaß an Inhalten, das alle Teilnehmenden unabhängig von Rolle oder späterem Spezialisierungsgrad beherrschen müssen. Diese Inhalte unterliegen nur seltenen, wohl begründeten Anpassungen. Die Aktualisierungsbausteine bilden dagegen eine flexible Schicht, die

regelmäßig überprüft und bei Bedarf angepasst oder ergänzt wird. Hier können neue Szenarien, Fallstudien, Tools oder Schwerpunktthemen aufgenommen, bestehende Inhalte aktualisiert oder obsolet gewordene Elemente reduziert werden, ohne dass das Fundament des Curriculums jedes Mal neu gebaut werden muss. Organisatorisch wird dies durch einen einfachen, aber verbindlichen Review-Prozess abgesichert. Beispielsweise kann jährlich (oder nach größeren Übungen/Einsätzen) ein Gremium aus Fach- und Ausbildungsexpert:innen zusammentreten, um zu prüfen:

- Welche neuen Bedrohungen, Technologien oder organisatorischen Entwicklungen sind seit der letzten Überarbeitung relevant geworden?
- Welche Lessons Learned aus Übungen, realen Vorfällen oder multinationalen Zusammenarbeitserfahrungen sollten curricular verankert werden?
- Welche Szenarien, Fallstudien oder Playbooks haben sich bewährt, welche müssen aktualisiert oder ersetzt werden?
- Sind die Grundlagemodule weiterhin stimmig oder bestehen Anpassungsbedarfe, etwa durch technologische Strukturänderungen (z. B. verstärkte Cloud-Nutzung, neue Führungsinformationssysteme)?

Solche Prozesse werden in der Literatur zu Cybersecurity-Bildung und -Professionalität als Teil eines „Curriculum Lifecycle Management“ empfohlen, das Planung, Implementierung, Evaluation und Revision systematisch verbindet. [129] Für militärisches SOC- und NOC-Personal hat dieser aktualitäts- und zukunftsorientierte Ansatz schließlich auch eine operative Dimension: Er unterstützt die Fähigkeit, neue Technologien und Taktiken nicht nur passiv nachzuvollziehen, sondern aktiv zu bewerten und sinnvoll in bestehende Strukturen einzupassen. Das Curriculum bereitet die Teilnehmenden darauf vor, etwa neue Sensorik, neue Analytik-Verfahren, Automatisierungsansätze oder neue Kooperationsformen mit Partnern kritisch zu prüfen, Chancen und Risiken abzuwägen und Vorschläge für deren Integration in nationale und multinationale Strukturen zu erarbeiten. Damit wird Aktualität nicht mit kurzfristiger Trendorientierung verwechselt, sondern als strategisch gesteuerte Weiterentwicklung verstanden, die sich an Auftrag, Resilienz und langfristiger Handlungsfähigkeit der Streitkräfte ausrichtet.

5.5.7 Präsenzorientierung mit Offline-Selbststudium

Alle Ausbildungsanteile dieses Curriculums werden bewusst in Präsenz durchgeführt. Diese Entscheidung ist zum einen sicherheits- und geheimhaltungsbedingt: Der Umgang mit sensiblen Informationen, die Nutzung geschützter Infrastrukturen sowie der Betrieb militärischer und ggf. klassifizierter Cyber-Ranges setzen in vielen Fällen eine kontrollierte physische Umgebung voraus. Zum anderen entspricht die Präsenzorientierung den Anforderungen an Teamarbeit, nonverbale Kommunikation und unmittelbare Interaktion, wie sie im militärischen Alltag von SOC und NOC üblich sind. Studien zu Face-to-Face-Lernumgebungen zeigen, dass insbesondere für komplexe, kooperative Aufgaben – etwa gemeinsames Problemlösen, Entscheidungsfindung unter Zeitdruck oder das Einüben von Kommunikationsmustern – die direkte physische Zusammenarbeit Vorteile bietet, etwa durch schnellere Klärung von Missverständnissen, reichhaltigere Rückmeldesignale und eine stärkere soziale Kohäsion. [132] Präsenzformate erleichtern zudem die Einbindung in militärische Übungsumgebungen, die Nutzung der Cyber Range und die Kopplung an andere Ausbildungs- und Übungsvorhaben, etwa Stabsrahmenübungen oder verbundene Operationstrainings. Gleichzeitig trägt das Curriculum dem Umstand Rechnung, dass die Zielgruppen erwachsene Lernende mit heterogenen Vorerfahrungen sind. Andragogische Ansätze betonen, dass erwachsene Personen einen ausgeprägten Wunsch nach Selbststeuerung und nach der Möglichkeit haben, Lernprozesse an ihre eigenen Bedürfnisse und Erfahrungen anzuknüpfen. [133] Um dieses individuelle Lernen zu unterstützen, werden systematisch Offline-Unterlagen

bereitgestellt: Skripte, Reader, Checklisten, Übungsaufgaben und Nachschlagewerke. Diese Materialien stehen unabhängig von einer Online-Infrastruktur zur Verfügung – ein wichtiger Aspekt in sicherheitskritischen Umgebungen – und dienen der Vorbereitung (z. B. vor Kursbeginn), der Wiederholung (zwischen Modulen) und der Vertiefung (nach Übungen). Die Grundidee entspricht damit in abgeschwächter Form dem Prinzip des „flipped classroom“: Basale Wissensanteile und Wiederholungen werden in die Selbststudiumsphase verlagert, während die wertvolle Präsenzzeit für Anwendung, Diskussion, praktische Übungen und Reflexion genutzt wird. [134], [135]

Auf diese Weise können die Teilnehmenden Grundlagen im Selbststudium erarbeiten oder auffrischen, bevor sie in der Präsenzphase in komplexere, szenariobasierte Aufgaben einsteigen. Forschung zum flipped classroom und zu selbstreguliertem Lernen zeigt, dass eine solche Aufteilung – Vorbereitung vor der Veranstaltung, Anwendung und Vertiefung in der Veranstaltung – Lernleistungen verbessern kann, sofern die vorbereitenden Materialien klar strukturiert sind und die Präsenzzeit konsequent für aktive Lernformen genutzt wird. [135], [136] Für das hier beschriebene Curriculum bedeutet das: Präsenzveranstaltungen konzentrieren sich auf das, was sich schwer in Einzelarbeit abbilden lässt – gemeinsame Lageanalysen, Teamentscheidungen, Simulationen in der Cyber Range, Rollenspiele, Debriefings – während Informationsvermittlung und Wiederholung stärker in die Selbststudiumsphase verlagert werden. Der Mehrwert dieser Kombination liegt in einer effizienten Nutzung der Präsenzzeit und in einer gewissen individuellen Flexibilisierung, ohne auf Online-Lernen angewiesen zu sein. Unterschiedliche Vorkenntnisse können besser ausgeglichen werden: Teilnehmende mit geringerer Erfahrung nutzen die Selbststudiumsunterlagen, um Basiswissen aufzubauen, während erfahrenere Personen die Materialien zur Vertiefung nutzen oder selektiv Schwerpunkte setzen. Konzepte der selbstgesteuerten bzw. selbstgerichteten Lernens (Self-Directed Learning) betonen, dass Erwachsene davon profitieren, wenn sie Ziele, Tempo und Vertiefungstiefe in einem gewissen Rahmen selbst steuern können – vorausgesetzt, sie werden durch geeignete Strukturen, Materialien und Rückmeldeschleifen unterstützt. [130], [137] Das Curriculum schafft diesen Rahmen, indem es klare Lernziele, nachvollziehbare Lernpfade und anwendungsnahe Aufgaben bereitstellt. Gleichzeitig werden die Nachteile und Risiken dieser Konzeption bewusst adressiert. Im Vergleich zu Online-Formaten ist die zeitliche und räumliche Flexibilität von Präsenzformaten geringer; Dienstpläne, Einsatzverpflichtungen und räumliche Verfügbarkeit müssen sorgfältig berücksichtigt werden. Zudem besteht – wie bei allen Formen des Selbststudiums – die Gefahr, dass vorbereitende Materialien nicht oder nur unzureichend genutzt werden. Studien zum flipped classroom und zur selbstregulierten Lernpraxis zeigen, dass genau hier oft der Engpass liegt: Wenn Vorbereitungsphasen nicht klar in den Gesamtprozess eingebunden sind, bleibt ihre Nutzung zufällig, und die erhofften Effekte auf die Qualität der Präsenzzeit bleiben aus. [136] Um dies zu vermeiden, wird die Verbindung zwischen Vorbereitungsmaterial und Präsenzphasen im Curriculum klar gestaltet. Vorwissen aus den Unterlagen wird in Übungen vorausgesetzt und in geeigneter Form überprüft, etwa durch kurze Eingangsaufgaben, Quizze, Reflexionsfragen oder den Bezug auf konkrete vorbereitende Inhalte in Szenarien. Aufgaben in der Präsenzphase knüpfen direkt an die Offline-Materialien an, sodass der Nutzen der Vorbereitung für die Teilnehmenden transparent wird. Auf diese Weise entsteht ein impliziter Anreiz, die Unterlagen tatsächlich zu nutzen, da sie die Bearbeitung praktischer Aufgaben erleichtern und die aktive Teilnahme an Übungen ermöglichen. Ergänzend dazu ermöglicht eine vorausschauende Kursplanung eine bessere Vereinbarkeit mit dienstlichen Anforderungen: Lernfenster für Selbststudium werden bewusst eingeplant und kommuniziert, und die Verteilung von Präsenzblöcken berücksichtigt Einsatz-, Schicht- und Übungsplanung.

In der Summe kombiniert dieser Ansatz die Stärken präsenzorientierter Ausbildung – hohe Interaktionsdichte, unmittelbares Feedback, realitätsnahe Teamarbeit, sichere Umgebungen – mit den Vorteilen strukturierter Selbstlernphasen, wie sie in der Erwachsenenbildung und in flipped-classroom-Ansätzen als wirksam belegt sind. Präsenzorientierung mit Offline-Selbststudium ist

damit kein Rückschritt hinter moderne E-Learning-Konzepte, sondern eine bewusste, sicherheits- und auftragskonforme Adaption evidenzbasierter Lehr-Lern-Modelle an den militärischen SOC-/NOC-Kontext.

5.5.8 Ethik- und wertebasierte Philosophie

Schließlich beruht das Curriculum auf einer expliziten ethik- und wertebasierten Philosophie. Militärische Entscheidungen im Cyber- und Informationsraum haben nicht nur technische, sondern immer auch rechtliche, politische und gesellschaftliche Dimensionen. Cyber-Operationen können, je nach Zielwahl, Intensität und Kontext, Auswirkungen auf Zivilbevölkerung, kritische Infrastrukturen, Partnerstaaten oder das Vertrauen in staatliche Institutionen haben. Sie bewegen sich im Spannungsfeld von Landes- und Bündnisverteidigung, Landesrecht, Völkerrecht (insbesondere jus ad bellum und jus in bello) sowie menschenrechtlichen und humanitären Normen, wie sie u. a. im Tallinn Manual 2.0 systematisch auf die Cyber-Domäne angewendet werden. Eine Ausbildung, die diese Dimensionen ausblendet und Cyber-Sicherheit ausschließlich als technische Disziplin behandelt, wäre unvollständig, kurzfristig und im Zweifel selbst ein Risiko für Rechtskonformität, Legitimität und strategische Wirkung. Rechtliche Rahmenbedingungen, nationales Recht, Völkerrecht, militärische Vorschriften, Rules of Engagement, interne Weisungen – sowie ethische Fragestellungen wie Verhältnismäßigkeit, Kollateraleffekte, Schutz Unbeteiligter oder der verantwortungsvolle Umgang mit sensiblen Daten werden deshalb nicht in ein isoliertes „Ethik-Modul“ ausgelagert, sondern quer durch alle Ausbildungsphasen integriert. Dieser Ansatz folgt aktuellen Empfehlungen aus der Literatur zur Cybersecurity-Ausbildung, wonach Ethik nicht als einmalige Zusatzveranstaltung, sondern als durchgängiges Leitmotiv verankert werden sollte. Konkret bedeutet dies, dass in Fallstudien, Cyber-Range-Debriefings und Planspielen systematisch Situationen analysiert werden, in denen mehrere technisch mögliche Handlungsoptionen zur Verfügung stehen, die rechtlich und ethisch unterschiedlich zu bewerten sind. Beispiele sind etwa:

- die Frage, ob und wann Gegenmaßnahmen (z. B. aktives Blocking, Segmentierung, „Hackback“-ähnliche Maßnahmen) im Lichte von Rules of Engagement und Völkerrecht zulässig und verhältnismäßig sind,
- der Umgang mit kompromittierten Systemen, die sowohl militärische als auch zivile Funktionen erfüllen,
- die Frage, wie mit gewonnenen Daten umzugehen ist, wenn sie personenbezogene oder politisch sensible Informationen enthalten,
- die Abwägung zwischen operativer Effektivität und dem Risiko unbeabsichtigter Nebenwirkungen auf Zivilbevölkerung oder Partnerstaaten.

Die Teilnehmenden sollen in solchen Szenarien lernen, Dilemmata zu erkennen, relevante rechtliche und ethische Kriterien zu identifizieren, Abwägungen transparent zu begründen und bei Unsicherheit aktiv Rechtsberatung oder fachliche Unterstützung einzuholen. Forschung zu Cyber-Ethik und just-war-orientierten Analysen von Cyber-Operationen unterstreicht, dass klassische Kriterien wie Notwendigkeit, Verhältnismäßigkeit, Unterscheidung/Distinktion und Verantwortung auch in der Cyberdomäne anwendbar sind – aber bewusst gemacht und eingeübt werden müssen.

Ein zentrales Ziel dieser ethik- und wertebasierten Ausrichtung ist die Ausbildung einer reflektierten professionellen Identität, in der technische Exzellenz, Auftragserfüllung und Verantwortungsbewusstsein gegenüber Recht und Werten zusammengehören. Dies knüpft an neuere Ansätze einer wertebasierten Cybersecurity an, die betonen, dass Sicherheitsentscheidungen immer Wertentscheidungen sind – etwa im Hinblick auf Sicherheit vs. Freiheit, Transparenz vs. Geheimhaltung, Effizienz vs. Sorgfalt. Das Curriculum zielt darauf ab,

SOC- und NOC-Personal nicht nur dazu zu befähigen, technisch „richtige“ Maßnahmen umzusetzen, sondern auch dazu, diese im Lichte der rechtlichen und ethischen Rahmenbedingungen kritisch zu reflektieren und gegebenenfalls zu korrigieren. Dies stärkt auf mehreren Ebenen die Qualität operativer Entscheidungen: Erstens reduziert es das Risiko von Maßnahmen, die zwar technisch effizient, aber rechtlich problematisch oder politisch kontraproduktiv sind. Zweitens verbessert es die Argumentations- und Kommunikationsfähigkeit gegenüber Vorgesetzten, Rechtsberatern und politischen Entscheidungsträgern, weil Entscheidungen besser begründet werden können. Drittens trägt es zum Vertrauen von Öffentlichkeit, Politik und Partnern in die Streitkräfte als verantwortungsvollen Akteur im Cyber- und Informationsraum bei – ein Aspekt, der in Debatten um militärische Cyberoperationen immer wieder hervorgehoben wird.

Didaktisch folgt das Curriculum den Erkenntnissen, dass Ethik besonders wirksam vermittelt wird, wenn sie fall- und szenariobasiert umgesetzt wird. Arbeiten zu Cybersecurity-Ethikcurricula zeigen, dass realistische Fallstudien und die Diskussion konkreter Dilemmata deutlich wirkungsvoller sind als rein regelbasierte oder rein abstrakte „Ethikvorlesungen“. Daher werden rechtlich-ethische Fragestellungen in typische Lernformate integriert:

- in Fallstudien, in denen aus der Perspektive von SOC-/NOC-Personal, Stäben oder Rechtsberatung Entscheidungen vorbereitet und begründet werden,
- in Cyber-Range-Debriefings, in denen neben technischen und prozessualen Aspekten auch die rechtlich-ethische Bewertung des Handelns besprochen wird („Welche Optionen wären rechtlich zulässig gewesen?“, „War das Vorgehen verhältnismäßig?“),
- in Planspielen und Stabsübungen, in denen die Einbindung von Rechtsberater:innen, politischen Vorgaben und Rules of Engagement simuliert und praktisch eingeübt wird.

Mögliche Nachteile dieser ethik- und wertebasierten Ausrichtung werden ebenfalls bewusst adressiert. In der Praxis werden ethische Inhalte von manchen Teilnehmenden – insbesondere in technisch geprägten Berufsbildern – als „weich“, „nicht prüfungsrelevant“ oder nachrangig gegenüber „harter Technik“ wahrgenommen. Studien zur Integration von Ethik in Informatik- und Cybersecurity-Curricula bestätigen diese Wahrnehmung und zeigen, dass Ethikmodule oft geringere Verbindlichkeit und Sichtbarkeit haben als technische Fächer. Um dem entgegenzuwirken, verfolgt das Curriculum mehrere Strategien:

- Integration in bewertete Aufgaben: Rechtlich-ethische Aspekte werden nicht nur „nebenbei“ thematisiert, sondern sind Bestandteil bewerteter Leistungsnachweise – etwa in Szenariobearbeitungen, schriftlichen Lagebeurteilungen, Kurzvorträgen oder Reflexionsaufgaben. Bewertet wird nicht „moralische Gesinnung“, sondern die Fähigkeit, relevante Normen zu erkennen, Alternativen zu benennen und eine nachvollziehbare, regelkonforme Begründung zu liefern. Das signalisiert, dass Ethik kein Zusatzthema, sondern Teil professioneller Kompetenz ist.
- Verbindliche Reflexionsphasen: Für jede größere Übung – insbesondere Cyber-Range-Übungen und komplexe Planspiele – sind verbindliche, wenn auch kurze, Reflexionsphasen vorgesehen. Dort werden ausdrücklich Fragen gestellt wie: „Welche rechtlichen Rahmenbedingungen waren relevant?“, „Gab es ethische Spannungsfelder?“, „Welche Alternativen hätte es gegeben?“ Diese Reflexion wird als fester Bestandteil des Übungsformats verankert, nicht als optionales Add-on.
- Vorbildfunktion der Lehrenden: Lehrende und Instruktor:innen werden darauf vorbereitet, rechtlich-ethische Aspekte aktiv anzusprechen und vorzuleben, statt sich ausschließlich auf technische Inhalte zu konzentrieren. Literatur zur Wertebildung und zur Rolle von



„communities of practice“ zeigt, dass Vorbilder und gelebte Praxis einen erheblichen Einfluss darauf haben, ob Werte tatsächlich in der Berufskultur ankommen.

Auf diese Weise bleibt die ethische Dimension inhaltlich wie formal ein fester Bestandteil des Curriculums. Sie wird nicht nur in Leitbildern oder Zielbeschreibungen erwähnt, sondern ist in konkrete Lernziele, Methoden, Szenarien und Prüfungsformate übersetzt. Für militärisches SOC- und NOC-Personal bedeutet dies, dass sie nicht nur technisch auf dem aktuellen Stand ausgebildet werden, sondern auch als verantwortliche Akteure im Cyber- und Informationsraum, die ihre Entscheidungen an Recht, Werten und Auftrag ausrichten können – und dies im Zweifel auch gegenüber Vorgesetzten, Partnern und Öffentlichkeit begründen können.

5.6 Struktur des Curriculums

Die Struktur des Curriculums folgt dem didaktischen Grundsatz einer progressiven Kompetenzentwicklung: von gemeinsamen Grundlagen über gemeinsame operationelle Fähigkeiten hin zu rollenbezogener Spezialisierung und abschließender Integrationsleistung. Ein solcher Aufbau ist aus curriculartheoretischer Sicht zweckmäßig, weil er verhindert, dass Lernende entweder zu früh in hochspezialisierte Themenfelder eintreten oder über einen zu langen Zeitraum auf einer abstrakten, von konkreten Handlungssituationen entkoppelten Basisebene verbleiben. Die Architektur des Curriculums dient somit nicht allein der inhaltlichen Ordnung, sondern der systematischen Herstellung von Anschlussfähigkeit zwischen Ausbildung, dienstlicher Verwendung und langfristiger Fähigkeitsentwicklung.

Zugleich ist die Struktur so konzipiert, dass Kompetenzaufbau nachvollziehbar, überprüfbar und in den militärischen Dienstbetrieb rückkoppelbar bleibt. Dies ist für SOC- und NOC-bezogene Qualifizierungsarchitekturen von besonderer Bedeutung, da hier nicht nur deklaratives Wissen, sondern vor allem handlungsfähige, lagebezogene und kooperationsrelevante Kompetenz aufgebaut werden muss. Die curriculare Gliederung schafft daher eine Ordnungslogik, in der Lernziele, Ausbildungsformate, Leistungsnachweise und Rollenprofile in ein kohärentes Verhältnis gesetzt werden. Gleichzeitig wird eine Anschlussfähigkeit an arbeitsplatznahe Kompetenz- und Rollenmodelle hergestellt, wie sie in internationalen Cyber-Workforce-Frameworks beschrieben werden [138], [139], [140]. Das Curriculum orientiert sich damit nicht nur an pädagogischen Überlegungen, sondern auch an funktionalen Erfordernissen militärischer Cyber- und Netzbetriebsorganisationen.

5.6.1 Didaktische Progression als leitendes Strukturprinzip

Das erste leitende Strukturmerkmal des Curriculums ist die didaktische Progression. Darunter ist in der Bildungswissenschaft die planvolle und sachlogisch begründete Abfolge von Lernschritten zu verstehen, durch die Lernende von grundlegenden Kenntnissen schrittweise zu einer belastbaren und anwendungsfähigen Kompetenz gelangen. Progression bedeutet in diesem Zusammenhang nicht lediglich, dass Inhalte „nacheinander“ vermittelt werden. Vielmehr beschreibt sie einen systematischen Aufbau, bei dem frühere Lerninhalte die Voraussetzung für spätere, komplexere Anforderungen bilden. Ein Curriculum mit didaktischer Progression ist daher so gestaltet, dass Lernende nicht mit isolierten Einzelinformationen konfrontiert werden, sondern einen nachvollziehbaren Lernpfad durchlaufen, in dem Wissen aufgebaut, vertieft, angewandt und schließlich in komplexen Handlungssituationen integriert wird.

Im vorliegenden Curriculum erfolgt diese Progression nicht linear im Sinne einer bloßen Aneinanderreihung von Themenblöcken, sondern sequenziell, kumulativ und vertiefend. „Sequenziell“ bedeutet, dass die Inhalte in einer begründeten Reihenfolge angeordnet sind. „Kumulativ“ bedeutet, dass neu erworbenes Wissen auf bereits vorhandenen Kenntnissen aufbaut und diese nicht ersetzt, sondern erweitert. „Vertiefend“ bedeutet schließlich, dass zentrale Konzepte nicht nur einmal behandelt, sondern im weiteren Verlauf erneut aufgegriffen und unter anspruchsvolleren Bedingungen angewendet werden. Auf eine gemeinsame konzeptionelle Grundlage folgen zunächst anwendungsorientierte operationelle Wissensgebiete. Daran schließen rollenbezogene Vertiefungen an, in denen die Lernenden spezifische Anforderungen ihrer späteren Aufgabenprofile bearbeiten. Den Abschluss bilden integrative Übungs- und Prüfungsformate, in denen Wissen unter realitätsnahen Bedingungen vernetzt, beurteilt und praktisch umgesetzt werden muss. Die curriculare Struktur folgt damit einem Lernverständnis, das auf nachhaltigen Kompetenzaufbau und nicht auf kurzfristige Wissensreproduktion abzielt.

Um dieses Strukturprinzip verständlich zu machen, ist eine nähere Erklärung des Begriffs Kompetenz erforderlich. Kompetenz bezeichnet nicht bloß das Vorhandensein von Wissen,

sondern die Fähigkeit, Wissen, Fertigkeiten, Urteilsvermögen und Haltung in konkreten Situationen angemessen einzusetzen. Von operationeller Handlungskompetenz ist dann zu sprechen, wenn Personen in der Lage sind, in realen oder realitätsnahen Einsatz- und Betriebssituationen sachgerecht, zielorientiert und verantwortungsvoll zu handeln. Im Kontext eines militärischen Curriculums für den Cyber- und Informationsraum bedeutet dies, dass Lernende nicht nur technische Begriffe kennen oder Verfahrensschritte auswendig wiedergeben, sondern komplexe Lagen erkennen, Informationen bewerten, Prioritäten setzen, Entscheidungen vorbereiten, mit anderen Akteuren kommunizieren und ihr Handeln an übergeordneten Aufträgen und Rahmenbedingungen ausrichten können. Handlungskompetenz ist daher immer mehrdimensional: Sie umfasst kognitive, praktische, kommunikative und organisationsbezogene Elemente.

Didaktisch ist die gewählte Abfolge deshalb zweckmäßig, weil sie dem Umstand Rechnung trägt, dass militärisches Personal im Cyber- und Informationsraum nicht nur technische Einzelkenntnisse benötigt, sondern komplexe Zusammenhänge erkennen, strukturieren und in koordiniertes Handeln überführen können muss. In hochdynamischen und häufig von Unsicherheit geprägten Lagen reicht es nicht aus, einzelne Fachinformationen isoliert zu beherrschen. Erforderlich ist vielmehr die Fähigkeit, unterschiedliche Informationsquellen zusammenzuführen, ihre Relevanz einzuschätzen, Handlungsoptionen abzuleiten und diese in einem organisatorischen und oftmals hierarchisch geprägten Umfeld umzusetzen. Die didaktische Progression trägt dieser Anforderung Rechnung, indem sie Lernende zunächst in zentrale Begriffe, Modelle und Grundprinzipien einführt, bevor diese Grundlagen in operationellen Kontexten konkretisiert und schließlich in spezialisierten Aufgabenbereichen vertieft werden. Damit wird vermieden, dass Lernende entweder von Beginn an mit zu komplexen, stark spezialisierten Situationen überfordert werden oder umgekehrt auf einer rein theoretischen Ebene verbleiben, ohne den praktischen Sinn der vermittelten Inhalte zu verstehen.

Ein zentrales Merkmal dieses Ansatzes ist, dass Lernen als Entwicklungsprozess verstanden wird. Die Ausbildung beginnt mit einer gemeinsamen konzeptionellen Orientierung. Diese Phase dient dazu, ein einheitliches Verständnis zentraler Begriffe und Zusammenhänge herzustellen. Gerade in interdisziplinären Tätigkeitsfeldern wie SOC- und NOC-Strukturen ist dies unverzichtbar, weil eine gemeinsame Sprache die Voraussetzung für Zusammenarbeit, Lageverständnis und konsistente Entscheidungsfindung ist. Erst auf dieser Grundlage können anwendungsorientierte Wissensgebiete sinnvoll vermittelt werden. In diesen wird das zuvor erworbene Grundwissen in konkretere Handlungszusammenhänge überführt, etwa durch die Auseinandersetzung mit Monitoring, Alarmierung, Analyse, Störungsbearbeitung oder Reaktionsprozessen. Die anschließenden rollenbezogenen Vertiefungen ermöglichen es dann, die unterschiedlichen Anforderungen spezifischer Tätigkeitsprofile gezielt auszubilden. Integrative Übungs- und Prüfungsformate stellen schließlich sicher, dass die erworbenen Kenntnisse nicht fragmentiert bleiben, sondern in komplexen Szenarien unter Zeitdruck, Unsicherheit und Koordinationsbedarf angewendet werden. Aus lernpsychologischer Sicht ist diese Progression deshalb besonders wirksam, weil nachhaltiges Lernen in der Regel nicht durch einmalige Informationsaufnahme entsteht. Wissen wird erst dann stabil und handlungswirksam, wenn es mehrfach aktiviert, in unterschiedlichen Kontexten genutzt und mit praktischen Erfahrungen verknüpft wird. Kompetenz entsteht in diesem Zusammenhang nicht allein durch die Aufnahme von Informationen, sondern durch die wiederholte Verbindung von Fachwissen, Lageverständnis, Entscheidungsfähigkeit und Kommunikationsleistung. Fachwissen liefert die begrifflichen und sachlichen Grundlagen. Lageverständnis ermöglicht es, eine Situation in ihrem Zusammenhang zu erfassen und ihre Relevanz einzuschätzen. Entscheidungsfähigkeit beschreibt die Fähigkeit, unter Unsicherheit und Zeitdruck sachgerechte Optionen zu entwickeln und Prioritäten zu setzen. Kommunikationsleistung wiederum ist notwendig, um Beobachtungen, Bewertungen und Handlungsbedarfe so zu vermitteln, dass sie im Team, in übergeordneten Führungsstrukturen oder in angrenzenden

Fachbereichen wirksam werden. Erst das Zusammenspiel dieser Dimensionen führt zu jener Form von Professionalität, die für militärisches Handeln im Cyber- und Informationsraum erforderlich ist.

Die didaktische Progression des Curriculums zielt daher darauf ab, Lernende schrittweise von der konzeptuellen Orientierung zur selbstständigen, rollenadäquaten Handlung zu führen. Konzeptuelle Orientierung bedeutet, dass Lernende zunächst verstehen, welche Begriffe, Modelle, Prozesse und Prinzipien ihrem späteren Handeln zugrunde liegen. Rollenadäquate Handlung bedeutet demgegenüber, dass sie diese Grundlagen in der jeweils eigenen Funktion sachgerecht anwenden können. Dieser Übergang von Verständnis zu Anwendung ist ein Kernelement professioneller Ausbildung. Er ist besonders relevant in militärischen Kontexten, in denen Aufgaben selten rein theoretisch bearbeitet werden, sondern fast immer in organisationale Abläufe, Kommunikationsketten und lageabhängige Entscheidungsprozesse eingebettet sind. Ein Curriculum, das diesen Übergang nicht systematisch vorbereitet, würde Gefahr laufen, zwar Wissen zu vermitteln, aber keine hinreichende Einsatzbefähigung zu erzeugen. Darüber hinaus erhöht die didaktische Progression nicht nur die fachliche Kohärenz der Ausbildung, sondern auch ihre praktische Wirksamkeit in dienstlichen Verwendungen. Fachliche Kohärenz bedeutet, dass die einzelnen Bestandteile des Curriculums inhaltlich aufeinander abgestimmt sind und ein nachvollziehbares Ganzes bilden. Praktische Wirksamkeit bedeutet, dass das Gelernte in realen Arbeits- und Einsatzkontexten tatsächlich nutzbar wird. Beide Ziele sind eng miteinander verbunden. Nur wenn Lernende erkennen, wie einzelne Inhalte zusammenhängen und aufeinander aufbauen, können sie diese Inhalte in neuen Situationen flexibel anwenden. Für militärische Ausbildungszusammenhänge ist dies von besonderer Bedeutung, weil dort nicht die isolierte Beherrschung einzelner Themen, sondern die zuverlässige Erfüllung komplexer Aufgaben im Vordergrund steht.

Didaktische Progression ist weit mehr als ein formales Ordnungsprinzip. Sie bildet das pädagogische Grundgerüst des Curriculums. Durch die geordnete, aufbauende und vertiefende Struktur wird sichergestellt, dass aus Grundlagenwissen schrittweise eine belastbare Handlungskompetenz entsteht, die unter realitätsnahen Bedingungen wirksam werden kann. Gerade im militärischen Cyber- und Informationsraum, in dem technisches Verständnis, Lagebezug, Kommunikationsfähigkeit und koordiniertes Handeln eng miteinander verflochten sind, ist eine solche progressive Curriculumslogik eine wesentliche Voraussetzung für professionelle und einsatzfähige Ausbildung.

5.6.2 Die vier Ebenen der Curriculumsstruktur

Strukturell gliedert sich das Curriculum in vier aufeinander bezogene Ebenen: erstens in die Basisausbildung, zweitens in gemeinsame operationelle Wissensgebiete, drittens in rollenbezogene Vertiefungsmodule für SOC und NOC und viertens in integrative Abschlussübungen und Leistungsnachweise. Diese vier Ebenen sind nicht als voneinander getrennte oder isolierte Ausbildungsblöcke zu verstehen, sondern als Entwicklungsstufen innerhalb eines konsistenten Qualifizierungssystems. Die curriculare Logik besteht darin, dass jede Ebene auf den Ergebnissen der vorhergehenden aufbaut, diese vertieft und in einen neuen Anwendungszusammenhang überführt. Auf diese Weise entsteht ein geordneter Kompetenzpfad, der von grundlegender Orientierung über operationelle Befähigung bis hin zur selbstständigen und koordinierten Handlung in realitätsnahen Lagen reicht.

Ein solcher Aufbau ist aus bildungswissenschaftlicher und berufspädagogischer Sicht besonders zweckmäßig, weil professionelle Handlungskompetenz in komplexen Tätigkeitsfeldern nicht punktuell oder sprunghaft entsteht. Sie entwickelt sich vielmehr schrittweise durch das Zusammenspiel von Wissensaufbau, Übung, Reflexion, Spezialisierung und Anwendung. Für militärische Funktionen im SOC- und NOC-Umfeld ist dies von besonderer Bedeutung, da diese Rollen nicht nur technisches Fachwissen, sondern auch Lageverständnis, Priorisierungsfähigkeit,

Koordinationsvermögen und die Fähigkeit zur belastbaren Kommunikation unter Zeitdruck verlangen. Die vier Ebenen des Curriculums bilden somit nicht lediglich eine organisatorische Gliederung, sondern einen systematischen Rahmen zur Entwicklung belastbarer beruflicher und operationeller Kompetenz.

5.6.2.1 Basisausbildung als gemeinsames begriffliches und konzeptionelles Fundament

Die Basisausbildung schafft ein gemeinsames Fundament an Begriffen, Denkmodellen und sicherheitsbezogenen Grundprinzipien. Ihre Funktion besteht darin, zunächst jene konzeptionellen Voraussetzungen herzustellen, ohne die eine weiterführende operationelle oder spezialisierte Ausbildung nicht konsistent möglich wäre. In dieser Phase geht es nicht primär um die Bearbeitung hochkomplexer Einzelfälle, sondern um die Ausbildung eines gemeinsamen Verständnisses von Sicherheit, Risiko, Schutzbedarfen, Rollenverantwortung, Identitäts- und Zugriffsmanagement, Richtlinienarchitekturen sowie von grundlegenden Betriebs- und Sicherheitslogiken.

Der Begriff des gemeinsamen Fundaments ist dabei wörtlich zu verstehen. In militärischen Umfeld, in den Personal aus unterschiedlichen Vorbildungen, Teilorganisationen und Erfahrungsräumen zusammenkommt, ist ein einheitliches Begriffsverständnis keine Nebensache, sondern eine Voraussetzung wirksamer Zusammenarbeit. Begriffe wie „Risiko“, „Vorfallsbearbeitung“, „Verfügbarkeit“, „Integrität“, „Schutzbedarf“ oder „Eskalation“ dürfen nicht nur oberflächlich bekannt sein, sondern müssen im gleichen Sinn verstanden werden. Nur dann können Lagebewertungen, Meldungen, Entscheidungen und Reaktionen organisationsweit anschlussfähig bleiben. Die Basisausbildung stiftet deshalb eine gemeinsame Sprache, die es erlaubt, technische Sachverhalte, sicherheitsrelevante Beobachtungen und organisatorische Anforderungen in konsistenter Form zu erfassen und zu kommunizieren. Darüber hinaus vermittelt diese erste Ebene grundlegende Denkmodelle. Dazu gehört etwa das Verständnis, dass Sicherheit nicht als statischer Zustand, sondern als fortlaufender Prozess der Prävention, Erkennung, Bewertung und Reaktion zu begreifen ist. Ebenso zentral ist die Einsicht, dass technische Systeme immer in organisatorische, personelle und regelgebundene Kontexte eingebettet sind. Sicherheitsprobleme entstehen daher nicht ausschließlich durch technische Schwächen, sondern häufig durch das Zusammenwirken von Technik, Prozessen, Rollenunklarheiten, Fehlkonfigurationen und unzureichender Kommunikation. Eine fundierte Basisausbildung muss deshalb technische, organisatorische und normative Elemente miteinander verbinden.

5.6.2.2 Gemeinsame operationelle Wissensgebiete als Brücke zwischen Grundlagen und Praxis

Die zweite Ebene umfasst gemeinsame operationelle Wissensgebiete. Hier werden die zuvor eingeführten Grundlagen in konkrete operationelle Kontexte überführt. Diese Ebene besitzt eine Brückenfunktion: Sie verbindet die eher begrifflich-konzeptionelle Basisausbildung mit den späteren, stärker spezifizierten Rollenanforderungen im SOC- und NOC-Bereich. Während auf der ersten Ebene vor allem Orientierungswissen aufgebaut wird, zielt die zweite Ebene darauf ab, dieses Wissen in Handlungslogiken zu überführen, die in beiden Rollenräumen relevant sind.

Zu diesen gemeinsamen operationellen Wissensgebieten zählen unter anderem Monitoring, Alarmierung, Ereigniskorrelation, Incident Response, System- und Netzwerkverständnis, Datenaufbereitung sowie forensische Grundlogiken. Diese Themen sind deshalb gemeinsam zu vermitteln, weil sowohl SOC- als auch NOC-Personal mit der Beobachtung, Einordnung und Bearbeitung sicherheits- oder betriebsrelevanter Ereignisse befasst ist, auch wenn sich die konkreten Schwerpunktsetzungen später unterscheiden. Ein grundlegendes Verständnis von Monitoring bedeutet hier beispielsweise nicht nur zu wissen, dass Systeme überwacht werden, sondern auch zu verstehen, welche Datenquellen dafür relevant sind, wie Schwellenwerte,

Auffälligkeiten und Indikatoren interpretiert werden und wie aus technischer Beobachtung operationell relevante Information wird. Ähnliches gilt für den Begriff der Ereigniskorrelation. Darunter ist die Verknüpfung mehrerer Einzelbeobachtungen zu einem zusammenhängenden Lagebild zu verstehen. In operationellen Umgebungen treten Störungen, Warnhinweise und Anomalien selten in isolierter Form auf. Ihre Bedeutung erschließt sich häufig erst aus dem Zusammenhang mehrerer Datenpunkte. Das Curriculum muss daher vermitteln, wie Einzelereignisse systematisch zusammengeführt, priorisiert und bewertet werden können. Dies ist nicht nur eine technische, sondern auch eine analytische Kompetenz, da aus einer Vielzahl potenziell relevanter Informationen jene Muster erkannt werden müssen, die auf eine Störung, einen Angriff oder eine kritische Betriebsentwicklung hindeuten.

Die Funktion dieser zweiten Ebene besteht insgesamt darin, eine gemeinsame operationelle Handlungslogik herzustellen, bevor eine differenzierte Spezialisierung erfolgt. Aus didaktischer Sicht ist dies wesentlich, weil Spezialisierung nur dann sinnvoll ist, wenn zuvor ein gemeinsamer Rahmen besteht, innerhalb dessen unterschiedliche Rollen anschlussfähig bleiben. Ein SOC ohne Verständnis für betriebliche Abhängigkeiten oder ein NOC ohne Verständnis für detektions- und lagebezogene Prozesse würde die Zusammenarbeit erschweren. Die gemeinsame operationelle Ebene legt daher die Grundlage für arbeitsteilige, aber dennoch koordinierte Handlung.

5.6.2.3 Rollenbezogene Vertiefungsmodule als funktionale Ausdifferenzierung

Die dritte Ebene beinhaltet rollenbezogene Vertiefungsmodule. In dieser Phase erfolgt die gezielte Ausdifferenzierung jener Kompetenzen, die für spezifische Funktionsprofile erforderlich sind. Diese Spezialisierung ist notwendig, weil SOC- und NOC-Rollen zwar auf gemeinsamen Grundlagen beruhen, im operationellen Alltag jedoch unterschiedliche Primäraufgaben, Beobachtungslogiken und Entscheidungserfordernisse aufweisen.

Im SOC stehen detektionsorientierte, analysebezogene und lagebildrelevante Kompetenzen im Vordergrund. Dazu gehören insbesondere die strukturierte Analyse von Sicherheitsereignissen, die Bewertung von Indikatoren und Warnsignalen, die Korrelation verteilter Beobachtungen, die Priorisierung von Vorfällen, die Entwicklung erster Hypothesen zu Ursache und Reichweite eines Ereignisses sowie die Erstellung adressatengerechter Lageinformationen. Das SOC arbeitet somit stärker an der Schnittstelle zwischen technischer Erkennung, analytischer Einordnung und koordinierter Reaktion. Seine Tätigkeit ist besonders stark auf Mustererkennung, Unsicherheitsbewältigung und die Übersetzung technischer Beobachtungen in entscheidungsrelevante Information ausgerichtet.

Die NOC-Vertiefung fokussiert demgegenüber stärker auf Betriebsstabilität, Netzwerkinfrastruktur, Servicekontinuität, Fehlermanagement sowie auf netzwerk- und OT-nahe Aufgabenstellungen. Hier steht weniger die primäre Detektion sicherheitsrelevanter Angriffsmuster als vielmehr die Sicherstellung eines stabilen, resilienten und nachvollziehbar betriebenen technischen Gesamtsystems im Vordergrund. Dazu zählen etwa das Verständnis von Netzsegmentierung, Konfigurationsabhängigkeiten, Fehlerursachen, Wiederherstellungslogiken, Verfügbarkeitsanforderungen und die Bewertung betrieblicher Auswirkungen technischer Anomalien. Das NOC benötigt somit eine besonders ausgeprägte Kompetenz für Systemzusammenhänge, Betriebskontinuität und technische Wiederherstellung unter einsatznahen Bedingungen.

Die Spezialisierung baut auf einem gemeinsamen Fundament auf, ohne die notwendige Differenzierung der Aufgabenprofile zu vernachlässigen. Gerade darin liegt ihre curriculare Stärke. Sie verhindert einerseits, dass Rollenprofile künstlich vermischt werden, und stellt andererseits sicher, dass Spezialisierung nicht zur Abschottung führt. Für militärische Einsatz- und Betriebsrealitäten ist dies von hoher Bedeutung, weil Wirksamkeit häufig nicht aus isolierter

Exzellenz einzelner Teilbereiche entsteht, sondern aus der koordinierten Zusammenarbeit spezialisierter Funktionen.

5.6.2.4 Integrative Abschlussübungen und Leistungsnachweise als Nachweis handlungsfähiger Kompetenz

Die vierte Ebene umfasst integrative Abschlussübungen und Leistungsnachweise. Hier werden die zuvor aufgebauten Kenntnisse und Fertigkeiten unter zeitkritischen, realitätsnahen und kooperationsintensiven Bedingungen zusammengeführt. Diese Ebene markiert den Übergang von der modularen Wissensvermittlung zur ganzheitlichen Anwendungsleistung und besitzt damit eine besondere curriculare Funktion. Sie prüft nicht nur, ob Lernende Inhalte reproduzieren können, sondern ob sie in der Lage sind, unter komplexen Bedingungen fachlich fundiert, priorisiert und koordiniert zu handeln.

Integrative Übungen sind deshalb unverzichtbar, weil Handlungskompetenz sich nicht vollständig in Einzelprüfungen oder rein theoretischen Leistungsnachweisen abbilden lässt. In realen oder realitätsnahen Lagen müssen Informationen oft unter Zeitdruck bewertet, Unsicherheiten kommuniziert, konkurrierende Prioritäten abgewogen und Entscheidungen unter unvollständiger Datenlage vorbereitet werden. In solchen Situationen zeigt sich, ob Lernende Fachwissen tatsächlich in Lageverstehen, Priorisierung, Kommunikation und koordiniertes Handeln überführen können. Gerade für militärische Verwendungskontexte ist dies zentral, da dort das isolierte Beherrschen technischer Inhalte allein nicht ausreicht. Erforderlich ist vielmehr die Fähigkeit, in einem organisatorischen Gefüge handlungswirksam zu werden. Leistungsnachweise auf dieser Ebene sollten daher mehrdimensional angelegt sein. Sie müssen nicht nur Fachrichtigkeit erfassen, sondern auch die Qualität von Lageeinschätzungen, die Nachvollziehbarkeit von Entscheidungen, die Einhaltung von Eskalationswegen, die Zusammenarbeit im Team und die adressatengerechte Kommunikation berücksichtigen. Erst eine solche mehrdimensionale Bewertung wird dem Anspruch gerecht, militärische Einsatzbefähigung und nicht bloß Wissensbesitz zu prüfen.

5.6.3 Kompetenzaufbau und Wiederaufnahme zentraler Konzepte

Aus didaktischer Perspektive ist die Struktur des Curriculums als spiralförmig zu beschreiben. Mit diesem Begriff ist gemeint, dass zentrale Konzepte nicht einmalig behandelt und anschließend abgeschlossen werden, sondern im Verlauf der Ausbildung wiederholt aufgegriffen, erweitert und in neue Anwendungszusammenhänge überführt werden. Das Curriculum folgt damit nicht dem Prinzip einer linearen Stoffabfolge, bei der ein Thema nach seiner Behandlung endgültig verlassen wird. Stattdessen werden wesentliche Begriffe und Handlungsmuster mehrfach aufgegriffen, wobei jede Wiederaufnahme mit einer höheren fachlichen Tiefe, einem komplexeren Anwendungskontext oder einer größeren Selbstständigkeit der Lernenden verbunden ist. Begriffe wie Risiko, Angriffserkennung, Eskalation, Resilienz, Verfügbarkeit, Integrität, Lagebild, Anomalie oder Reaktionskette erscheinen deshalb nicht nur in einem einzelnen Modul, sondern auf unterschiedlichen Niveaustufen und unter wechselnden Perspektiven. So kann etwa der Begriff Risiko zunächst in der Basisausbildung als Grundbegriff der Sicherheitslogik eingeführt werden. In späteren operationellen Modulen wird er dann auf konkrete Bedrohungs- und Ausfallkonstellationen bezogen. In spezialisierten Phasen wird Risiko weiter als Kriterium für Priorisierung, Eskalationsentscheidungen und Ressourceneinsatz konkretisiert. In Abschlussübungen wiederum zeigt sich, ob Lernende in der Lage sind, unter Zeitdruck zu erkennen, welche Risiken handlungsleitend sind und wie diese kommuniziert werden müssen. Das gleiche Prinzip gilt für andere Kernbegriffe: Sie gewinnen im Verlauf des Curriculums an Tiefe, Kontextbezug und Handlungsrelevanz. Diese spiralförmige Struktur ist für die Ausbildung in militärischen SOC- und NOC-Kontexten besonders geeignet, weil sie nachhaltiges Lernen begünstigt. Komplexe operationelle Handlungskompetenz entsteht in der Regel nicht durch

einmalige Vermittlung, sondern durch wiederholte Auseinandersetzung mit denselben Grundprinzipien in wachsender fachlicher Tiefe. Wissen, das zunächst begrifflich verstanden wurde, wird anschließend prozessual eingeordnet, später in Fallanalysen angewendet und schließlich unter Belastungsbedingungen geübt. Dieser Übergang von der begrifflichen Erfassung über die analytische Einordnung bis hin zur handlungsbezogenen Anwendung ist für professionelle Ausbildung grundlegend. Er trägt dem Umstand Rechnung, dass Lernende komplexe Inhalte meist nicht in einem einzigen Schritt vollständig durchdringen, sondern diese in mehreren Durchgängen zunehmend differenziert verstehen.

Darüber hinaus fördert die spiralförmige Struktur den Transfer von Wissen in neue Kontexte. Transfer bedeutet, dass Gelerntes nicht nur in genau der Form wiedergegeben werden kann, in der es vermittelt wurde, sondern auch in veränderten Situationen nutzbar wird. Gerade dies ist für militärische Cyber- und Netzbetriebsrollen entscheidend, da reale Lagen selten identisch mit Trainingssituationen sind. Wer Konzepte nur einmal und in einem engen Zusammenhang kennengelernt hat, wird Schwierigkeiten haben, sie auf neue Konstellationen zu übertragen. Werden dieselben Konzepte jedoch wiederholt unter verschiedenen Perspektiven behandelt, steigt die Wahrscheinlichkeit, dass Lernende deren allgemeinen Kern erkennen und flexibel anwenden können. Für die curriculare Planung bedeutet dies, dass einzelne Module nicht isoliert entwickelt werden dürfen. Vielmehr muss jedes Modul erkennbar machen, an welche zuvor vermittelten Inhalte es anschließt, welche Elemente es vertieft und welche Anwendungsdimensionen neu hinzukommen. Ein Modul ist in diesem Verständnis nicht nur eine in sich geschlossene Lerneinheit, sondern Teil eines größeren Entwicklungspfad. Diese Anbindung muss sowohl inhaltlich als auch didaktisch sichtbar sein: in der Formulierung von Lernzielen, in der Auswahl von Übungsformaten, in der Gestaltung von Leistungsnachweisen und in der Benennung von Anschlussstellen zu früheren und späteren Modulen.

Auf diese Weise wird ein nachvollziehbarer Kompetenzpfad erzeugt, der sowohl für Lernende als auch für Ausbildungsplanende transparent bleibt. Für Lernende erhöht dies die Orientierung im Ausbildungsprozess, da sie erkennen können, warum bestimmte Inhalte wiederkehren und wie sich ihr Kompetenzniveau schrittweise entwickelt. Für Ausbildungsplanende schafft die spiralförmige Struktur die Möglichkeit, Redundanzen von produktiver Wiederaufnahme zu unterscheiden. Nicht jede Wiederholung ist didaktisch sinnvoll; sinnvoll ist sie dann, wenn sie auf einer neuen Stufe stattfindet, neue Perspektiven eröffnet und zu einer erweiterten Anwendungsfähigkeit führt. Die Spirale ist daher nicht als bloßes Wiederholen desselben zu verstehen, sondern als systematische Vertiefung und Kontextualisierung.^{3.4} Gemeinsames Fundament und differenzierte Rollenbildung

Ein zentrales Strukturprinzip des Curriculums ist die Trennung zwischen gemeinsamem Fundament und differenzierter Rollenbildung. Diese Trennung ist aus fachlicher wie organisationaler Sicht notwendig. Militärische SOC- und NOC-Teams arbeiten im Betrieb eng zusammen, verfolgen jedoch nicht identische Zielsetzungen, priorisieren unterschiedliche Indikatoren und agieren auf Grundlage teilweise unterschiedlicher operationeller Logiken. Ein wirksames Curriculum muss daher zwei Anforderungen zugleich erfüllen: Es muss einerseits ein gemeinsames Begriffs-, Prozess- und Lageverständnis herstellen und andererseits eine funktional angemessene Differenzierung der Rollen ermöglichen. Das gemeinsame Fundament hat dabei eine integrierende Funktion. Es stellt sicher, dass Sicherheitsprinzipien, Eskalationsmechanismen, Meldewege, Reaktionslogiken, Lagebildbegriffe und Kommunikationsformen organisationsweit konsistent verstanden werden. Dies ist gerade in militärischen Umgebungen von hoher Bedeutung, weil dort Entscheidungen häufig unter Zeitdruck, in hierarchischen Strukturen und mit mehreren beteiligten Organisationseinheiten getroffen werden müssen. Fehlende gemeinsame Begriffe oder uneinheitliche Prozessvorstellungen würden in solchen Lagen unmittelbar zu Reibungsverlusten, Missverständnissen und Verzögerungen führen.

Die differenzierte Rollenbildung setzt an diesem Fundament an. Im SOC werden insbesondere detektions- und intelligence-orientierte Kompetenzen vertieft, etwa im Bereich Analyse von Sicherheitsereignissen, Bewertung von Indikatoren, Korrelation von Meldungen und Erstellung lagebezogener Bewertungen. Im NOC stehen dagegen betriebs- und infrastrukturorientierte Kompetenzen stärker im Vordergrund, beispielsweise in Bezug auf Netzwerkverfügbarkeit, Servicequalität, Konfigurationskontrolle, Fehlerdiagnose, Schnittstellenmanagement und gegebenenfalls OT-nahe Betriebsanforderungen. Die curriculare Differenzierung trägt somit der realen Aufgabenverteilung Rechnung, ohne die Kooperation zwischen beiden Rollenräumen zu schwächen.

5.6.4 Verbindung von Wissensgebieten, Modulen und Qualifikationsstufen

Ein weiteres grundlegendes Strukturprinzip des Curriculums ist die systematische Verbindung von Wissensgebieten, Modulen und Qualifikationsstufen. Diese Dreigliederung ist curriculardidaktisch besonders leistungsfähig, weil sie drei unterschiedliche, aber eng miteinander verknüpfte Ebenen professioneller Ausbildung unterscheidbar macht: erstens die Frage, was gelernt werden soll, zweitens wie dieses Lernen organisiert und vermittelt wird, und drittens, mit welcher Tiefe, Selbstständigkeit und Handlungsfähigkeit die Lernenden die jeweiligen Inhalte beherrschen sollen. Die Stärke dieses Ansatzes liegt darin, dass fachliche Inhalte, didaktische Umsetzung und erwartetes Leistungsniveau nicht vermischt, sondern systematisch aufeinander bezogen werden. Dadurch entsteht eine belastbare Struktur, die sowohl für die Planung als auch für die Durchführung, Evaluation und Weiterentwicklung des Curriculums von hohem Nutzen ist.

5.6.4.1 Wissensgebiete als fachliche Domänen der Ausbildung

Wissensgebiete definieren die fachlichen Domänen, die im Rahmen der Ausbildung beherrscht werden müssen. Sie beantworten die grundlegende curriculare Frage, welche thematischen Felder für die Zielrollen relevant sind und welche fachlichen Grundlagen, Zusammenhänge und Problemstellungen daher systematisch behandelt werden müssen. Im vorliegenden Kontext umfassen solche Wissensgebiete etwa Netzwerkgrundlagen, Monitoring, Incident Handling, forensische Basisprinzipien, Richtlinienumsetzung, Kommunikationsprozesse, rechtliche Rahmenbedingungen, Identitäts- und Zugriffsmanagement, Systemverständnis oder lagebezogene Analyseverfahren. Didaktisch betrachtet erfüllen Wissensgebiete mehrere Funktionen. Erstens strukturieren sie den fachlichen Gegenstandsbereich der Ausbildung und verhindern, dass Inhalte nur zufällig oder anlassbezogen vermittelt werden. Zweitens schaffen sie Transparenz darüber, welche Kompetenzen zu einem bestimmten Rollenprofil gehören und welche fachlichen Zusammenhänge für das Verständnis operationeller Aufgaben unverzichtbar sind. Drittens ermöglichen sie eine curriculare Priorisierung: Nicht jedes denkbare Spezialthema muss in gleicher Intensität behandelt werden, wohl aber jene fachlichen Domänen, die für die angestrebte Handlungsfähigkeit konstitutiv sind. Wissensgebiete bilden damit gewissermaßen die inhaltliche Landkarte des Curriculums. Sie benennen nicht nur Themen, sondern markieren den Raum professioneller Expertise, innerhalb dessen sich die Ausbildung bewegt.

Gerade im militärischen Cyber- und Informationsraum ist diese fachliche Strukturierung besonders bedeutsam. Die relevanten Aufgabenfelder sind durch technische Komplexität, dynamische Bedrohungslagen und hohe Interdependenz geprägt. Ohne eine klare Definition von Wissensgebieten bestünde die Gefahr, dass Ausbildung entweder zu unspezifisch bleibt oder sich zu stark an kurzfristigen Werkzeugen, Einzelfällen oder organisationslokalen Praktiken orientiert. Ein auf Wissensgebieten beruhendes Curriculum schafft demgegenüber ein übertragbares und stabileres Kompetenzfundament.

5.6.4.2 Module als didaktische und organisatorische Übersetzung fachlicher Inhalte

Module übersetzen diese Wissensgebiete in konkrete Lern- und Lehrarrangements. Während Wissensgebiete definieren, welche fachlichen Domänen beherrscht werden müssen, legen Module fest, wie diese Domänen in lernbare, überprüfbare und organisatorisch umsetzbare Einheiten überführt werden. Sie bestimmen, in welcher didaktischen Form Inhalte vermittelt werden, welche Reihenfolge zweckmäßig ist, welche Übungsanteile integriert werden und wie Lernfortschritt überprüft wird. Ein Modul ist daher nicht nur eine organisatorische Einheit im Stundenplan, sondern ein didaktisch begründeter Baustein, in dem Lernziele, Inhalte, Methoden, Übungen und Bewertungsformen aufeinander abgestimmt werden.

Für die Curriculumsentwicklung ist diese Ebene von besonderer Bedeutung, weil erst durch die modulare Struktur aus einem fachlichen Anspruch ein praktisch umsetzbares Ausbildungsformat entsteht. Module entscheiden darüber, ob Lernende Inhalte nur rezeptiv aufnehmen oder ob sie diese aktiv anwenden, reflektieren und transferieren müssen. Sie legen außerdem fest, ob ein Thema beispielsweise in Form von Vorträgen, problemorientierten Fallbearbeitungen, simulationsgestützten Sequenzen, kooperativen Arbeitsformaten oder praktischen Übungen vermittelt wird. Damit prägen Module wesentlich die Qualität des Lernprozesses. Zugleich erfüllen Module eine wichtige Steuerungsfunktion für militärische Ausbildungsorganisationen. Sie ermöglichen eine zeitliche und personelle Planbarkeit, erleichtern die Integration verschiedener Lehrender und schaffen die Voraussetzung dafür, Ausbildungsabschnitte flexibel zu kombinieren, zu aktualisieren oder in unterschiedlichen Lehrgangsformaten wiederzuverwenden. Ein modular aufgebautes Curriculum ist daher sowohl didaktisch als auch organisatorisch vorteilhaft: Es schafft Struktur, ohne die notwendige Anpassungsfähigkeit an unterschiedliche Rahmenbedingungen zu verlieren.

5.6.4.3 Qualifikationsstufen als Bestimmung von Tiefe, Selbstständigkeit und Verantwortungsgrad

Qualifikationsstufen bestimmen schließlich, in welcher Tiefe und mit welchem Grad an Selbstständigkeit eine Aufgabe oder ein Aufgabenbereich beherrscht werden soll. Sie beantworten damit die Frage, auf welchem Leistungsniveau Lernende ein Wissensgebiet oder Modul am Ende der Ausbildung beherrschen müssen. Dies ist insbesondere deshalb wichtig, weil fachliche Inhalte allein noch keine Aussage darüber erlauben, ob eine Person lediglich Begriffe reproduzieren, standardisierte Verfahren anwenden, komplexe Lagen selbstständig beurteilen oder in unsicheren Situationen verantwortliche Entscheidungen vorbereiten kann.

Aus curriculardidaktischer Sicht machen Qualifikationsstufen die Entwicklung von Handlungskompetenz sichtbar und bewertbar. Sie erlauben eine Differenzierung zwischen elementarem Verständnis, angeleiteter Anwendung, selbstständiger Bearbeitung und reflektierter, auch unter Belastung tragfähiger Professionalität. Im militärischen Kontext kommt hinzu, dass mit wachsender Qualifikationsstufe häufig auch ein erhöhter Verantwortungsgrad verbunden ist. Wer nicht nur technische Informationen aufnehmen, sondern Lagebilder verdichten, Eskalationsentscheidungen vorbereiten oder in Schicht- und Krisensituationen priorisieren soll, benötigt ein anderes Kompetenzniveau als Personen, die vor allem standardisierte Teilaufgaben unter Anleitung ausführen. Die Einbeziehung von Qualifikationsstufen erhöht daher die Präzision des Curriculums erheblich. Sie sorgt dafür, dass Ausbildung nicht bloß inhaltlich vollständig, sondern auch hinsichtlich ihres Anspruchsniveaus realistisch, differenziert und rollenadäquat gestaltet wird. Gleichzeitig erleichtert sie die Formulierung transparenter Leistungsnachweise und die Zuordnung von Ausbildungszielen zu späteren dienstlichen Verwendungen.

5.6.4.4 Curriculare und organisationale Bedeutung der Dreigliederung

Gerade für Ausbildungsumgebungen ist diese Dreigliederung von hohem Nutzen. Sie ermöglicht eine präzisere Zuordnung zwischen Ausbildungszielen und späteren dienstlichen Anforderungen. Dies ist deshalb bedeutsam, weil militärische Verwendungen im Cyber- und Informationsraum häufig durch arbeitsteilige Rollen, unterschiedliche Verantwortungsgrade und wechselnde operative Kontexte geprägt sind. Ein Curriculum, das Wissensgebiete, Module und Qualifikationsstufen systematisch miteinander verbindet, kann diese Vielfalt abbilden, ohne an Kohärenz zu verlieren. Darüber hinaus erleichtert diese Struktur die Anpassung des Curriculums an veränderte technische, organisationale oder operative Rahmenbedingungen. Werden beispielsweise neue Technologien relevant, können diese als Erweiterung eines Wissensgebiets aufgenommen werden, ohne die gesamte Curriculumstruktur neu aufbauen zu müssen. Werden Rollenprofile verändert oder ausdifferenziert, können Module angepasst oder Qualifikationsstufen neu justiert werden, ohne dass die Grundlogik des Curriculums infrage gestellt wird. Die Struktur schafft damit sowohl Stabilität als auch Entwicklungsfähigkeit. Gerade in einem dynamischen Umfeld wie dem Cyber- und Informationsraum ist diese Kombination von zentraler Bedeutung, weil Ausbildung zugleich belastbar und veränderungsoffen sein muss.

5.6.5 Verschränkung von Fachlichkeit und Anwendungsleistung

Ein drittes tragendes Strukturprinzip des Curriculums liegt in der bewussten Verschränkung von Fachlichkeit und Anwendungsleistung. Dieses Prinzip ist von zentraler Bedeutung, weil professionelle Ausbildung im sicherheits- und operationsbezogenen Umfeld nicht darauf reduziert werden kann, isoliertes Fachwissen zu vermitteln. Vielmehr muss sie darauf ausgerichtet sein, Wissen in Handlungskompetenz zu überführen. Fachlichkeit bezeichnet in diesem Zusammenhang die systematische Vermittlung von Begriffen, Konzepten, Methoden, Verfahren und fachlichen Zusammenhängen innerhalb eines bestimmten Gegenstandsbereichs. Sie schafft das inhaltliche und begriffliche Fundament, das notwendig ist, um sicherheitsrelevante, betriebliche und analytische Sachverhalte überhaupt erkennen, beschreiben und einordnen zu können. Anwendungsleistung meint demgegenüber die Fähigkeit, dieses Wissen in konkreten beruflichen und operationellen Situationen sachgerecht, situationsangemessen, verantwortungsvoll und zielgerichtet einzusetzen. Sie umfasst damit nicht nur die praktische Ausführung einzelner Schritte, sondern auch die Fähigkeit zur Beurteilung von Lagen, zur Priorisierung unter Zeitdruck, zur Abstimmung mit anderen Akteuren sowie zur begründeten Auswahl von Handlungsoptionen.

Das Curriculum folgt damit ausdrücklich nicht dem traditionellen Muster einer strikten Trennung von Theorie und Praxis, bei dem Fachwissen zunächst losgelöst von Handlungskontexten vermittelt und erst in einem nachgeordneten Schritt praktisch angewandt wird. Ein solches Modell erscheint für einfache oder stark standardisierte Ausbildungsgegenstände möglicherweise ausreichend, stößt jedoch dort an seine Grenzen, wo Handeln von Unsicherheit, Dynamik, Interdependenz und Zeitkritik geprägt ist. Gerade in militärischen SOC- und NOC-Kontexten ist Wissen nie bloß theoretischer Besitz, sondern stets in Beobachtung, Bewertung, Kommunikation, Priorisierung und Entscheidung eingebettet. Technische Inhalte entfalten ihren eigentlichen Sinn daher nicht losgelöst von realen oder realitätsnahen Anwendungssituationen, sondern erst im Kontext konkreter Problemstellungen, in denen Informationen unvollständig, Handlungsoptionen konkurrierend und Folgen von Fehlentscheidungen potenziell erheblich sind. Ein Curriculum, das Fachwissen ausschließlich abstrakt vermittelt, würde deshalb Gefahr laufen, dass Lernende zwar Begriffe, Methoden und Prozesse benennen können, deren funktionale Bedeutung und operative Relevanz jedoch nur unzureichend erfassen. Die bewusste curriculare Verbindung von Fachlichkeit und Anwendungsleistung trägt diesem Problem Rechnung, indem praktische Übungen, Fallstudien, simulationsgestützte Lernszenarien, Cyber-Range-Sequenzen und strukturierte Reflexionsphasen frühzeitig in den Lernverlauf integriert werden. Diese frühe Integration ist



didaktisch bedeutsam, weil sie Lernenden von Beginn an verdeutlicht, dass Fachwissen nicht Selbstzweck ist, sondern als Ressource für begründetes Handeln dient. Wissen wird dadurch nicht als statischer Vorrat abstrakter Informationen erlebt, sondern als Werkzeug zur Orientierung, Bewertung und Problemlösung in konkreten Lagen. Dies erhöht nicht nur den Kontextbezug und die Motivation, sondern verbessert auch die langfristige Verfügbarkeit des Gelernten. Inhalte, die wiederholt in Handlungssituationen eingebettet werden, werden in der Regel tiefer verarbeitet, besser erinnert und flexibler auf neue Kontexte übertragen als Inhalte, die ausschließlich deklarativ vermittelt werden. Didaktisch besonders relevant ist dabei die Einsicht, dass Lernen in diesem Kontext nicht auf den Modus des Erinnerns beschränkt bleiben darf. Erinnern bezeichnet primär die Reproduktion bereits aufgenommener Informationen. Professionelle Handlungskompetenz im Cyber- und Informationsraum verlangt jedoch deutlich mehr. Sie setzt voraus, dass Lernende relevante Signale erkennen, deren Bedeutung interpretieren, Lageentwicklungen einschätzen, Handlungsoptionen bewerten und Entscheidungen innerhalb eines organisatorischen Rahmens vorbereiten oder unterstützen können. Lernen vollzieht sich damit im Modus des Erkennens, Interpretierens, Bewertens und Entscheidens. Diese Form des Lernens ist für militärische SOC- und NOC-Rollen besonders bedeutsam, da dort standardisierte Routinen allein nur selten ausreichen. Vielmehr müssen Fachkräfte in der Lage sein, auf neuartige oder mehrdeutige Situationen zu reagieren, Informationslücken zu überbrücken, Unsicherheiten transparent zu machen und ihr Handeln mit übergeordneten Führungs- und Kommunikationsstrukturen abzustimmen.

Gerade in solchen Kontexten zeigt sich, dass die Qualität professionellen Handelns nicht allein am Umfang des verfügbaren Wissens gemessen werden kann, sondern an der Fähigkeit, dieses Wissen unter realen Bedingungen angemessen einzusetzen. Der Cyber- und Informationsraum ist durch hohe technologische Komplexität, dynamische Entwicklungen und enge Wechselwirkungen zwischen technischen, organisatorischen und personellen Faktoren gekennzeichnet. Vorfälle sind häufig mehrdeutig, ihre Ursachen nicht sofort erkennbar und ihre Auswirkungen nicht auf einen einzelnen Systembereich beschränkt. Daraus ergibt sich, dass Fachkräfte nicht nur einzelne Verfahren beherrschen, sondern auch Zusammenhänge herstellen, Prioritäten setzen und Entscheidungen in einem Umfeld vorbereiten müssen, das von Zeitdruck, Unsicherheit und Interdependenz geprägt ist. Die curriculare Verschränkung von Fachlichkeit und Anwendung zielt genau auf die Befähigung zu dieser Form professioneller Handlungssicherheit. Ein wesentlicher Effekt dieser Struktur liegt in der Förderung professioneller Urteilskraft. Unter Urteilskraft ist die Fähigkeit zu verstehen, in komplexen, offenen und nicht vollständig regelgebundenen Situationen sachgerechte Einschätzungen vorzunehmen und Handlungen auf der Basis fachlicher, organisatorischer und situativer Kriterien zu begründen. Urteilskraft unterscheidet sich dabei sowohl vom bloßen Faktenwissen als auch von rein routinisierten Verfahrensabläufen. Sie wird überall dort relevant, wo Situationen nicht vollständig vorhersehbar sind, wo mehrere Interpretationen möglich bleiben und wo Entscheidungen nicht allein auf Grundlage formaler Checklisten getroffen werden können. Im militärischen Cyber-Kontext betrifft dies etwa die Einordnung von Anomalien, die Bewertung von Eskalationsnotwendigkeiten, die Priorisierung konkurrierender Meldungen oder die Entscheidung, welche Informationen in welcher Form an wen kommuniziert werden müssen. Solche Leistungen setzen voraus, dass Fachwissen mit Lageverständnis, Kommunikationsvermögen und organisationsbezogenem Denken verbunden wird.

Aus curriculardidaktischer Perspektive bedeutet dies, dass Fachinhalte nicht nur systematisch, sondern auch handlungsorientiert strukturiert werden müssen. Es genügt nicht, Inhalte fachlich korrekt auszuwählen; sie müssen so vermittelt werden, dass ihre Bedeutung für reale Entscheidungs- und Handlungskontexte erkennbar wird. Das Curriculum schafft hierfür einen Rahmen, in dem Wissen kontinuierlich mit Handlungserfordernissen verschränkt wird. Übungen, Fallanalysen und simulationsbasierte Szenarien übernehmen dabei nicht die Funktion bloßer



Veranschaulichung, sondern bilden einen integralen Bestandteil des Kompetenzaufbaus. Sie ermöglichen es, dass Lernende Fachinhalte nicht nur aufnehmen, sondern in situativen Zusammenhängen prüfen, anwenden, reflektieren und weiterentwickeln. Auf diese Weise wird eine Lernarchitektur geschaffen, die den Übergang von theoretischem Verstehen zu praktisch belastbarer Handlungskompetenz systematisch vorbereitet. Damit leistet die Verschränkung von Fachlichkeit und Anwendungsleistung einen wesentlichen Beitrag zur Wirksamkeit des Curriculums. Sie erhöht die Wahrscheinlichkeit, dass erworbenes Wissen im Dienstbetrieb tatsächlich verfügbar, anschlussfähig und nutzbar bleibt. Zugleich fördert sie ein professionelles Selbstverständnis, das technisches Wissen nicht isoliert betrachtet, sondern als Teil eines umfassenderen Handlungszusammenhangs begreift, der Analyse, Kommunikation, Verantwortung und Kooperation einschließt. Für die Ausbildung militärischen Personals in SOC- und NOC-Rollen ist dies von besonderer Bedeutung, da Wirksamkeit in diesen Funktionen nicht allein durch technische Expertise entsteht, sondern durch die Fähigkeit, diese Expertise in komplexen, zeitkritischen und organisationsgebundenen Lagen handlungsfähig zu machen. In diesem Sinn ist die bewusste Verschränkung von Fachlichkeit und Anwendungsleistung nicht nur ein didaktisches Detail, sondern ein konstitutives Strukturprinzip eines Curriculums, das auf professionelle Einsatzbefähigung ausgerichtet ist.

5.6.6 Übergangsorientierung zwischen Ausbildung, Dienstbetrieb und Teamleistung

Ein weiteres wesentliches Strukturprinzip des Curriculums ist die bewusste Ausrichtung auf Übergänge. Mit Übergängen sind dabei nicht nur zeitliche oder organisatorische Wechsel zwischen einzelnen Ausbildungsabschnitten gemeint, sondern vor allem jene Schnittstellen, an denen erworbene Kenntnisse und Fähigkeiten in neue Kontexte überführt werden müssen. Dazu gehören Übergänge zwischen Ausbildungsphasen, zwischen unterschiedlichen Rollenprofilen, zwischen Friedensbetrieb und Übung beziehungsweise Einsatz sowie zwischen individueller Kompetenz und kollektiver Teamleistung. In militärischen Ausbildungszusammenhängen kommt diesen Übergängen eine besondere Bedeutung zu, weil Lernerfolg nicht allein daran gemessen werden kann, ob Einzelpersonen Wissen wiedergeben oder standardisierte Abläufe reproduzieren können. Entscheidend ist vielmehr, ob erworbene Kompetenzen in reale Arbeits-, Führungs- und Unterstützungskontexte übertragen und dort unter wechselnden Bedingungen wirksam gemacht werden können. Aus curriculardidaktischer Sicht ist die Betonung von Übergängen deshalb bedeutsam, weil Lernen nicht in dem Moment abgeschlossen ist, in dem ein Inhalt vermittelt oder geprüft wurde. Professionelle Handlungskompetenz zeigt sich erst dann in belastbarer Form, wenn Wissen, Fertigkeiten und Urteilsvermögen in unterschiedlichen Kontexten anschlussfähig bleiben. Gerade in komplexen militärischen Verwendungszusammenhängen besteht häufig eine Diskrepanz zwischen Lehrgangssituation und Einsatzwirklichkeit. Während Ausbildungssituationen in der Regel didaktisch strukturiert, zeitlich begrenzt und pädagogisch begleitet sind, sind reale Arbeits- und Einsatzsituationen von Zeitdruck, Mehrdeutigkeit, Priorisierungskonflikten, Personalwechseln und organisationalen Abhängigkeiten geprägt. Ein Curriculum, das diese Unterschiede nicht systematisch mitdenkt, würde Gefahr laufen, Wissen zu erzeugen, das zwar im Unterrichtskontext verfügbar, im operationellen Alltag jedoch nur eingeschränkt handlungswirksam ist.

Vor diesem Hintergrund schafft das Curriculum wiederkehrende Bezugspunkte, die als verbindende Elemente zwischen unterschiedlichen Lernorten, Rollen und Anwendungsräumen fungieren. Zu diesen Bezugspunkten zählen gemeinsame Begriffe, standardisierte Lagebildlogiken, Playbooks, Eskalationsmodelle, Bewertungsraster und Qualitätskriterien, die sich durch mehrere Module und Ausbildungsphasen hindurchziehen. Solche Elemente erfüllen eine stabilisierende Funktion, weil sie Kontinuität in einem ansonsten heterogenen Lern- und Handlungssystem erzeugen. Sie tragen dazu bei, dass Lernende nicht in jedem neuen

Ausbildungs- oder Einsatzkontext vollständig neue Ordnungsmuster aufbauen müssen, sondern auf bekannte Begriffe, Verfahren und Bewertungsmaßstäbe zurückgreifen können. Dadurch wird Orientierung geschaffen, und zugleich wird die Wahrscheinlichkeit erhöht, dass erworbene Kompetenzen in veränderten Situationen tatsächlich aktiviert und angewendet werden. Die Funktion dieser wiederkehrenden Bezugspunkte geht jedoch über bloße Orientierung hinaus. Sie schaffen zugleich eine gemeinsame Referenzbasis für Auszubildende, Lernende und Vorgesetzte. Dies ist insbesondere in militärischen Organisationen von Bedeutung, in denen Ausbildung, Dienstbetrieb und Führung nicht getrennte Sphären darstellen, sondern eng miteinander verbunden sind. Eine gemeinsame Referenzbasis erleichtert nicht nur die Vermittlung und Überprüfung von Lerninhalten, sondern auch die Rückkopplung zwischen Ausbildungsergebnissen und dienstlicher Verwendung. Wenn etwa Lagebildlogiken, Eskalationsmodelle oder Qualitätskriterien sowohl in der Ausbildung als auch im späteren Arbeitskontext anschlussfähig sind, entsteht eine höhere Konsistenz zwischen Lernen und Anwenden. Damit wird das Curriculum zu einem Instrument, das nicht nur Wissen vermittelt, sondern auch organisationsweite Handlungslogiken stützt. Die Übergangsorientierung besitzt darüber hinaus eine ausgeprägte organisationspraktische Relevanz. In militärischen SOC- und NOC-Strukturen müssen Kompetenzen häufig unter Bedingungen von Schichtbetrieb, Personalwechsel, lageabhängiger Priorisierung und interdisziplinärer Zusammenarbeit wirksam werden. Dies bedeutet, dass individuelle Qualifikation allein nicht ausreicht. Vielmehr müssen Kenntnisse und Fähigkeiten so ausgebildet werden, dass sie in Teamprozesse, Kommunikationsketten, Meldewege, Führungsunterstützung und kooperative Problemlösung eingebracht werden können. Gerade hier zeigt sich, dass militärische Professionalität nicht allein als Eigenschaft einzelner Personen verstanden werden kann, sondern immer auch eine kollektive und organisationale Dimension besitzt. Ein technisch versierter Akteur, der seine Erkenntnisse nicht in ein gemeinsames Lagebild überführen, nicht adressatengerecht kommunizieren oder nicht an bestehende Verfahren anschließen kann, wird nur begrenzt zur Gesamtwirksamkeit beitragen.

Besonders wichtig ist in diesem Zusammenhang der Übergang von individueller Kompetenz zu kollektiver Teamleistung. Viele Ausbildungsmodelle konzentrieren sich primär auf die Frage, was Einzelpersonen wissen und können. Für militärische SOC- und NOC-Strukturen reicht diese Perspektive jedoch nicht aus. Dort entsteht Wirksamkeit häufig erst durch das koordinierte Zusammenwirken mehrerer Rollen, Funktionen und Verantwortungsbereiche. Ein Lagebild wird kollektiv erzeugt, Prioritäten werden abgestimmt, Entscheidungen werden vorbereitet oder umgesetzt, und Reaktionen müssen häufig organisationsübergreifend koordiniert werden. Das Curriculum muss daher nicht nur individuelle Lernfortschritte adressieren, sondern auch Übergänge in kooperative, teambezogene und organisationsbezogene Leistungskontexte vorbereiten. Dies erfordert Ausbildungsformate, in denen Kommunikation, Koordination, Rollenverständnis und Schnittstellenkompetenz gezielt eingeübt werden. Auch der Übergang zwischen Friedensbetrieb und Übung beziehungsweise Einsatz ist in diesem Zusammenhang zentral. Im Routinebetrieb werden viele Prozesse unter vergleichsweise stabilen Bedingungen durchgeführt. In Übungen oder Einsätzen verändern sich diese Bedingungen jedoch häufig grundlegend: Zeitdruck steigt, Unsicherheiten nehmen zu, Prioritäten verschieben sich, Kommunikationswege verdichten sich und Entscheidungen erhalten eine andere Tragweite. Ein Curriculum, das nur auf den Normalbetrieb ausgerichtet ist, würde daher zentrale Anforderungen militärischer Einsatzrealität verfehlen. Die Übergangsorientierung des Curriculums trägt diesem Umstand Rechnung, indem sie Lernende nicht nur auf standardisierte Abläufe vorbereitet, sondern auch auf die Veränderung von Rahmenbedingungen, die in Übungs- und Einsatzkontexten typischerweise eintreten. Dadurch wird Ausbildung nicht auf Routinekompetenz beschränkt, sondern auf Anpassungs- und Handlungsfähigkeit unter veränderten Bedingungen ausgerichtet.

Aus einer übergeordneten Perspektive leistet die explizite Strukturierung von Übergängen einen wesentlichen Beitrag dazu, individuelle Qualifizierung in organisationale Einsatzfähigkeit zu

transformieren. Diese Transformation ist ein zentrales Ziel militärischer Ausbildung. Wissen und Fertigkeiten besitzen nur dann einen nachhaltigen Wert, wenn sie in Strukturen eingebettet werden können, in denen sie kollektiv wirksam werden. Das Curriculum übernimmt dabei eine vermittelnde Funktion: Es verbindet Lernprozesse mit dienstlichen Anforderungen, individuelle Kompetenzentwicklung mit Teamleistung und fachliche Qualifikation mit institutioneller Handlungsfähigkeit. Gerade in komplexen und dynamischen Domänen wie dem Cyber- und Informationsraum ist diese Vermittlungsfunktion unverzichtbar, weil dort technische Expertise, organisatorische Koordination und führungsbezogene Anschlussfähigkeit eng miteinander verflochten sind.

5.6.7 Strukturelle Bedeutung für Qualitätssicherung und Weiterentwicklung

Die Struktur des Curriculums erfüllt schließlich auch eine zentrale Funktion für Qualitätssicherung und Weiterentwicklung. Sie ist damit nicht nur ein Mittel zur Ordnung von Inhalten, sondern zugleich ein Steuerungsinstrument für die Sicherung, Überprüfung und Anpassung von Ausbildungsqualität. Eine klar definierte curriculare Architektur erleichtert nicht nur die Durchführung von Ausbildung, sondern auch deren Evaluation, Vergleichbarkeit und langfristige Weiterentwicklung. Dies ist insbesondere in komplexen Ausbildungsfeldern von Bedeutung, in denen fachliche Anforderungen, technologische Rahmenbedingungen und organisationale Bedarfe einem fortlaufenden Wandel unterliegen. Ein Curriculum kann seine Funktion als belastbarer Referenzrahmen nur dann dauerhaft erfüllen, wenn seine Struktur so angelegt ist, dass sie sowohl Verlässlichkeit als auch lernende Anpassung ermöglicht.

Aus curricular-didaktischer Perspektive besteht die besondere Leistung einer strukturierten Architektur darin, dass sie Ausbildungsbestandteile in ein nachvollziehbares Verhältnis zueinander setzt. Wenn Basiselemente, gemeinsame operationelle Wissensgebiete, rollenbezogene Spezialisierungen und integrative Leistungsnachweise in einer erkennbaren Ordnung aufeinander bezogen sind, wird sichtbar, welche Funktion ein bestimmter Ausbildungsabschnitt im Gesamtsystem erfüllt. Diese Transparenz ist eine wesentliche Voraussetzung für Qualitätssicherung. Nur wenn eindeutig beschrieben ist, welche Inhalte auf welcher Ebene vermittelt werden, welche Kompetenzen jeweils aufgebaut werden sollen und in welcher Weise diese überprüft werden, lässt sich belastbar beurteilen, ob das Curriculum seine Ziele erreicht. Qualitätssicherung setzt somit nicht erst bei der Leistungsmessung an, sondern bereits bei der strukturellen Klarheit des Curriculums selbst. Eine solche Klarheit erleichtert die Evaluation auf mehreren Ebenen. Zum einen können Stärken identifiziert werden, etwa dort, wo Ausbildungsinhalte, Methoden und Leistungsnachweise erkennbar kohärent aufeinander abgestimmt sind und die angestrebten Kompetenzen wirksam unterstützen. Zum anderen werden Lücken sichtbar, also Bereiche, in denen relevante Inhalte nicht hinreichend abgedeckt, Übergänge unzureichend vorbereitet oder Kompetenzanforderungen nicht angemessen operationalisiert sind. Darüber hinaus können auch Überfrachtungen gezielter erkannt werden. Gerade in dynamischen Fachfeldern besteht häufig die Tendenz, neue Anforderungen additiv in bestehende Curricula aufzunehmen, ohne ältere oder weniger prioritäre Bestandteile systematisch zu überprüfen. Eine klar gegliederte Struktur wirkt dieser Entwicklung entgegen, weil sie nachvollziehbar macht, wo Inhalte funktional notwendig sind, wo sich Redundanzen bilden und wo thematische Verdichtungen zulasten didaktischer Konsistenz entstehen. Die strukturierte Gliederung des Curriculums schafft damit die Grundlage für eine evidenzbasierte Weiterentwicklung der Ausbildung. Evidenzbasiert bedeutet in diesem Zusammenhang, dass Anpassungen nicht allein aufgrund situativer Eindrücke, punktueller Rückmeldungen oder kurzfristiger Reaktionen vorgenommen werden, sondern auf systematisch gewonnenen Erkenntnissen beruhen. Solche Erkenntnisse können aus Leistungsnachweisen, Übungsergebnissen, Beobachtungen aus dem Dienstbetrieb, Rückmeldungen von Lehrenden und Lernenden, Erkenntnissen aus Einsätzen oder aus der

Analyse neuer technischer und regulatorischer Entwicklungen gewonnen werden. Ein Curriculum, dessen Struktur klar gegliedert ist, ermöglicht es, solche Rückmeldungen gezielt zu verorten: Es wird erkennbar, ob ein Defizit auf ein unzureichend ausgearbeitetes Wissensgebiet, auf ein didaktisch ungeeignetes Modul, auf eine unklare Übergangslogik oder auf eine nicht mehr passende Qualifikationsanforderung zurückzuführen ist. Dadurch wird Weiterentwicklung nicht zu einem unsystematischen Nachjustieren, sondern zu einem reflektierten und qualitätsgesicherten Entwicklungsprozess.

Von besonderer Bedeutung ist in diesem Zusammenhang die institutionelle Robustheit des Curriculums. Darunter ist die Fähigkeit eines Curriculums zu verstehen, auch unter veränderten Rahmenbedingungen funktionsfähig, anschlussfähig und konsistent zu bleiben. Eine strukturierte Gliederung erhöht diese Robustheit, weil sie transparent macht, welche Inhalte und Kompetenzfelder den unverzichtbaren Kern der Ausbildung bilden, welche Themenbereiche vertieft oder differenziert werden können und an welchen Stellen organisationsspezifische Ergänzungen sinnvoll oder erforderlich sind. Damit wird das Curriculum weder zu einem starren Regelwerk noch zu einem beliebig veränderbaren Sammelsystem. Vielmehr entsteht ein Rahmen, der einen stabilen Kern mit geregelten Möglichkeiten der Anpassung verbindet. Gerade im Cyber- und Informationsraum ist diese Kombination aus Stabilität und Weiterentwicklungsfähigkeit von zentraler Bedeutung. Dieser Bereich ist durch hohe technologische Dynamik, kurze Innovationszyklen, sich wandelnde Angriffsformen und veränderte operative Anforderungen geprägt. Ein Curriculum, das zu stark auf kurzfristige Werkzeuge, konkrete Produkte oder momentane Bedrohungsbilder zugeschnitten ist, verliert rasch an Relevanz. Umgekehrt ist ein Curriculum, das ausschließlich auf abstrakte und zeitunabhängige Grundbegriffe setzt, möglicherweise nicht hinreichend nah an den realen Anforderungen des Dienst- und Einsatzbetriebs. Die strukturierte Curriculumsarchitektur ermöglicht hier einen Ausgleich: Sie hält grundlegende Kompetenzlogiken, sicherheitsbezogene Prinzipien und handlungsleitende Konzepte stabil, während sie zugleich Raum für die geregelte Aufnahme neuer Technologien, Verfahren, Rollenprofile und Bedrohungslagen schafft. Diese Balance ist eine wesentliche Voraussetzung für nachhaltige Ausbildungsqualität.

Die Qualitätssicherungsfunktion der Struktur betrifft nicht nur Inhalte, sondern auch die Vergleichbarkeit und Nachvollziehbarkeit von Ausbildung. In institutionellen und militärischen Kontexten ist es bedeutsam, dass Ausbildungsleistungen nicht allein subjektiv oder situationsabhängig bewertet werden, sondern auf klaren Maßstäben beruhen. Eine strukturierte curriculare Architektur trägt hierzu bei, indem sie Lernziele, Kompetenzbereiche und Prüfungslogiken sichtbar ordnet. Dadurch wird es möglich, Ausbildungsdurchgänge über die Zeit hinweg zu vergleichen, Anpassungen zu dokumentieren und den Zusammenhang zwischen curricularen Veränderungen und beobachtbaren Effekten besser zu analysieren. Qualitätssicherung wird so nicht als punktuelle Kontrollhandlung verstanden, sondern als kontinuierlicher Prozess der Beobachtung, Rückmeldung und Verbesserung. Zugleich schafft die Struktur Voraussetzungen für die gesteuerte Integration organisationsspezifischer Anforderungen. Militärische Ausbildungsrealitäten unterscheiden sich häufig hinsichtlich Verfügbarkeiten, technischer Infrastruktur, Geheimschutzanforderungen, Führungsorganisation, nationaler Verfahren oder spezifischer Einsatzprofile. Ein tragfähiges Curriculum muss deshalb einerseits standardisierbar genug sein, um Vergleichbarkeit und Verbindlichkeit zu gewährleisten, andererseits aber offen genug bleiben, um solche kontextabhängigen Besonderheiten sinnvoll zu integrieren. Die strukturierte Gliederung macht sichtbar, an welchen Stellen solche Ergänzungen den Kern des Curriculums sinnvoll erweitern und an welchen Stellen sie diesen möglicherweise überlagern oder verzerren würden. Auch darin liegt ein wichtiger Beitrag zur institutionellen Qualitätssicherung.

Schließlich ist zu betonen, dass Qualitätssicherung im vorliegenden Zusammenhang nicht als bloß administratives Kontrollinstrument zu verstehen ist. Sie ist vielmehr selbst Teil professioneller Fähigkeitsentwicklung. Ein Curriculum, das regelmäßig überprüft, reflektiert und angepasst wird, bildet nicht nur den aktuellen Stand von Anforderungen ab, sondern entwickelt sich gemeinsam mit den Organisationen und Aufgabenfeldern weiter, für die es konzipiert ist. Die curriculare Struktur stellt dafür den notwendigen Referenzrahmen bereit. Sie sorgt dafür, dass Veränderung nicht zu Beliebigkeit führt und Stabilität nicht in Erstarrung umschlägt. In diesem Sinn ist die Struktur des Curriculums nicht nur Ordnungsmittel, sondern ein wesentlicher Garant dafür, dass Ausbildung langfristig wirksam, belastbar und entwicklungsfähig bleibt.

5.6.8 Schlussfolgerung zur Curriculumsstruktur

Zusammenfassend ist die Struktur des Curriculums als didaktisch-progressive, funktionsorientierte und anwendungsnahe Ausbildungsarchitektur zu verstehen. Sie folgt nicht einer bloß formalen Gliederungslogik, sondern einer pädagogisch und organisationspraktisch begründeten Ordnungsstruktur, die darauf ausgerichtet ist, ausgehend von gemeinsamen Grundlagen schrittweise eine belastbare, rollenadäquate und einsatzfähige Handlungskompetenz aufzubauen. Das Curriculum verbindet dabei gemeinsame Basiselemente mit rollenbezogener Differenzierung, fachliche Wissensgebiete mit modularer Vermittlungslogik sowie individuelle Kompetenzentwicklung mit team- und organisationsbezogener Einsatzfähigkeit. Seine Struktur ist damit nicht nur als Mittel der Stoffverteilung zu begreifen, sondern als konzeptioneller Rahmen, in dem Lernen, Anwenden, Überprüfen und Weiterentwickeln systematisch aufeinander bezogen werden.

Die didaktisch-progressive Ausrichtung zeigt sich darin, dass das Curriculum Lernprozesse nicht als additive Anhäufung isolierter Inhalte versteht, sondern als gestuften Kompetenzaufbau. Grundlagenwissen bildet den Ausgangspunkt, wird in gemeinsamen operationellen Wissensgebieten anwendungsnäher gefasst, in rollenbezogenen Vertiefungen funktional ausdifferenziert und in integrativen Übungen schließlich unter realitätsnahen Bedingungen zusammengeführt. Diese Progressionslogik ist aus didaktischer Sicht besonders tragfähig, weil sie dem Umstand Rechnung trägt, dass professionelle Handlungskompetenz in militärischen SOC- und NOC-Kontexten nicht durch einmalige Wissensvermittlung entsteht, sondern durch schrittweise Vertiefung, wiederholte Anwendung und reflektierte Einordnung. Die Struktur des Curriculums erzeugt damit einen nachvollziehbaren Lernpfad, der Lernenden Orientierung bietet und zugleich sicherstellt, dass die einzelnen Ausbildungsbestandteile nicht nebeneinanderstehen, sondern aufeinander aufbauen. Die Funktionsorientierung der Curriculumsstruktur liegt darin, dass sie sich an realen Rollenprofilen, Aufgabenlogiken und Anforderungslagen militärischer SOC- und NOC-Verwendungen ausrichtet. Ausbildung wird damit nicht als abstrakte Fachvermittlung verstanden, sondern als Vorbereitung auf konkrete berufliche und operationelle Funktionen. Dies ist insbesondere im Cyber- und Informationsraum von Bedeutung, da dort technische Expertise allein nicht ausreicht. Vielmehr müssen Kenntnisse, Fähigkeiten und Urteilsvermögen in organisational eingebettete Handlungszusammenhänge überführt werden, in denen Beobachtung, Bewertung, Kommunikation, Eskalation und Koordination eng miteinander verbunden sind. Indem das Curriculum gemeinsame Handlungslogiken sichert und zugleich funktionale Spezialisierung ermöglicht, trägt es dazu bei, dass unterschiedliche Rollenprofile nicht isoliert nebeneinanderstehen, sondern koordiniert zusammenwirken können. Die Anwendungsnähe des Curriculums besteht darin, dass Wissen nicht als rein theoretischer Bestand behandelt wird, sondern von Beginn an in Bezug auf praktische Handlungsanforderungen vermittelt wird. Fachliche Inhalte werden durch Übungen, Fallstudien, simulationsgestützte Szenarien und integrative Leistungsnachweise mit realitätsnahen Anwendungskontexten verschränkt. Dadurch wird sichergestellt, dass Lernende nicht nur Inhalte erinnern, sondern diese auch in komplexen, dynamischen und teilweise mehrdeutigen Situationen erkennen, bewerten und verantwortungsvoll

anwenden können. Für militärische Ausbildungsziele ist dies von zentraler Bedeutung, weil die Qualität professionellen Handelns gerade dort sichtbar wird, wo technische Kenntnisse unter Zeitdruck, Unsicherheit und Kooperationsanforderungen in belastbare Entscheidungen und abgestimmte Reaktionen überführt werden müssen.

Ein besonderer Vorzug dieser Curriculumsarchitektur liegt darin, dass sie Ordnung schafft, ohne operative Realität zu vereinfachen. Curriculare Ordnung ist notwendig, um Lernziele, Inhalte, Module, Qualifikationsstufen und Leistungsnachweise transparent zu strukturieren. Gleichzeitig darf eine solche Ordnung nicht zu einer didaktischen Vereinfachung führen, die die tatsächliche Komplexität militärischer Cyber- und Netzbetriebsrealitäten ausblendet. Die Stärke des Curriculums liegt daher gerade in seiner Fähigkeit, Komplexität nicht zu eliminieren, sondern didaktisch bearbeitbar zu machen. Es reduziert Realität nicht auf schematische Idealabläufe, sondern schafft eine Lernarchitektur, in der Unsicherheit, Interdependenz, Dynamik und Kooperationsbedarf schrittweise erschlossen und handhabbar gemacht werden. Ebenso bedeutsam ist, dass die Struktur Spezialisierung ermöglicht, ohne die Notwendigkeit gemeinsamer Handlungslogiken aus dem Blick zu verlieren. In militärischen SOC- und NOC-Strukturen ist Spezialisierung unverzichtbar, da unterschiedliche Funktionen unterschiedliche Vertiefungen erfordern. Zugleich bleibt organisationale Wirksamkeit darauf angewiesen, dass diese Spezialisierungen auf einem gemeinsamen Fundament ruhen und durch kompatible Begriffe, Verfahren, Lagebildlogiken und Kommunikationsformen verbunden bleiben. Das Curriculum löst dieses Spannungsverhältnis, indem es ein gemeinsames Fundament mit differenzierten Vertiefungen verbindet. Dadurch wird einerseits fachliche Tiefe ermöglicht und andererseits die Gefahr vermieden, dass spezialisierte Rollen in voneinander getrennte Wissens- und Handlungskulturen auseinanderdriften.

Darüber hinaus schafft die Struktur des Curriculums nicht nur einen nachvollziehbaren Lernpfad für die Ausbildung von SOC- und NOC-Personal, sondern zugleich einen belastbaren Rahmen für Prüfung, Qualitätssicherung und langfristige Fähigkeitsentwicklung. Weil die einzelnen Ebenen des Curriculums klar aufeinander bezogen sind, können Lernfortschritte systematisch überprüft, Ausbildungsqualität evaluiert und Anpassungsbedarfe transparent identifiziert werden. Das Curriculum erfüllt damit nicht nur eine pädagogische, sondern auch eine institutionelle Funktion: Es bildet einen Referenzrahmen, der Ausbildung, Personalentwicklung und organisationsbezogene Fähigkeitsplanung miteinander verbindet. Gerade in einem dynamischen Feld wie dem Cyber- und Informationsraum, in dem sich Technologien, Bedrohungslagen und operative Anforderungen rasch verändern, ist eine solche strukturierte und zugleich entwicklungsfähige Architektur von besonderem Wert.

5.7 Wissensgebiete

Die Wissensgebiete bilden das inhaltliche Rückgrat des Curriculums, weil sie eine fachsystematische Ordnung schaffen, die unabhängig von konkreten Lehrgangsformaten, Kursdauern oder Produktlandschaften Bestand haben kann. Sie beantworten die Frage, welche Domänen militärisches SOC- und NOC-Personal verstehen und beherrschen muss, um in unterschiedlichen Organisations- und Einsatzkontexten wirksam handeln zu können. Ihre Gliederung erlaubt es, Inhalte transparent zu priorisieren, auf Rollen abzubilden und in wiederverwendbare Lernpfade zu überführen. Gerade in einem Umfeld, das durch technologische Dynamik, heterogene Systeme und wechselnde Bedrohungsmuster gekennzeichnet ist, ist eine solche stabile Wissensarchitektur unverzichtbar.

Gleichzeitig sind die Wissensgebiete nicht als starre Fächerkanons zu verstehen. Sie dienen vielmehr als Referenzsystem, um Lernziele, Module, Übungen, Leistungsnachweise und spätere Aktualisierungen kohärent auszurichten. Ihre Funktion besteht darin, eine gemeinsame Sprache zwischen Ausbildung, Personalentwicklung und operationellem Bedarf zu schaffen. In diesem Sinn verbinden sie curriculare Planung mit Fähigkeitsentwicklung: Sie definieren, worüber Personal verfügen muss, ohne die konkrete Umsetzung unnötig zu verengen. Damit schaffen sie die Voraussetzung dafür, Grundlagen, operationelle Kompetenzen, Spezialisierungen und optionale Vertiefungen konsistent aufeinander aufzubauen.

5.7.1 Systematik der Wissensgebiete

Die in den Modulabbildungen ausgewiesenen Knowledge Areas bilden das inhaltliche Rückgrat des Curriculums. Sie strukturieren die Ausbildung entlang klarer Kompetenzfelder und stellen sicher, dass Grundlagen, operative Fähigkeiten sowie spezialisierte Vertiefungen systematisch und nachvollziehbar aufgebaut werden.

Für jedes Wissensgebiet werden Zweck, innere Struktur sowie zentrale Lernergebnisse beschrieben. Dadurch entsteht ein konsistenter Referenzrahmen für die Basisausbildung, die gemeinsame operationelle Ausbildung von SOC und NOC sowie für SOC- und NOC-spezifische Vertiefungen.

TABELLE 13 METASTRUKTUR CURRICULUM

Bereich	Schwerpunkt	Charakter
Basisausbildung	Awareness, Governance, Risiko, Resilienz und Informationsschutz	Gemeinsames Grundlagenverständnis für alle weiteren Module
Gemeinsame operationelle Wissensgebiete	Systemlebenszyklus, SIEM, Incident Response, Überwachung und Analyse	Gemeinsames Fundament für SOC- und NOC-Personal in Modul 2
SOC-spezifische Wissensgebiete	Threat Intelligence, Anomalieerkennung, Lagebild, Informationskrieg und Interventionsplanung	Vertiefung für detektions- und lageorientierte Cyberverteidigung
NOC-spezifische Wissensgebiete	Netzwerkverkehr, OT-Architekturen, Standards und Angriffserkennung	Vertiefung für netzwerk- und betriebsorientierte Cyberverteidigung
Optionale Vertiefungen	Linux, Kryptographie und Penetration Testing	Bedarfsorientierte Ergänzung zur weiteren Professionalisierung

5.7.2 Knowledge Areas der Basisausbildung

Die Basisausbildung vermittelt jene Wissensgebiete, die für alle Teilnehmenden als gemeinsamer Unterbau erforderlich sind. Im Vordergrund stehen Identitäten, Verhalten, Richtlinien, Risiko, Klassifikation und grundlegende Resilienz- und Schutzmechanismen.

TABELLE 14 CURRICULUM MODULSTRUKTUR

Knowledge Area	Zuordnung laut Modulstruktur
Identity Management	Qualification Level I Fundamentals
Awareness and Understanding	Qualification Level I Fundamentals
Social and Behavioral Privacy	Qualification Level I Fundamentals
Policy and Compliance Management	Qualification Level I Fundamentals
Security Governance	Qualification Level I Fundamentals
Compliance Monitoring and Reporting	Qualification Level I Fundamentals
Risk Management	Qualification Level I Fundamentals
Cybersecurity Planning	Qualification Level I Fundamentals
Cybersecurity Resilience	Qualification Level II Fundamentals
Information and Asset Classification	Qualification Level II Fundamentals
Security Evaluation Models	Qualification Level II Fundamentals
Security Capabilities of Information Systems	Qualification Level II Fundamentals
Embedded Devices and Cyber-physical System Vulnerability	Qualification Level II Fundamentals
Data Security	Qualification Level II Fundamentals

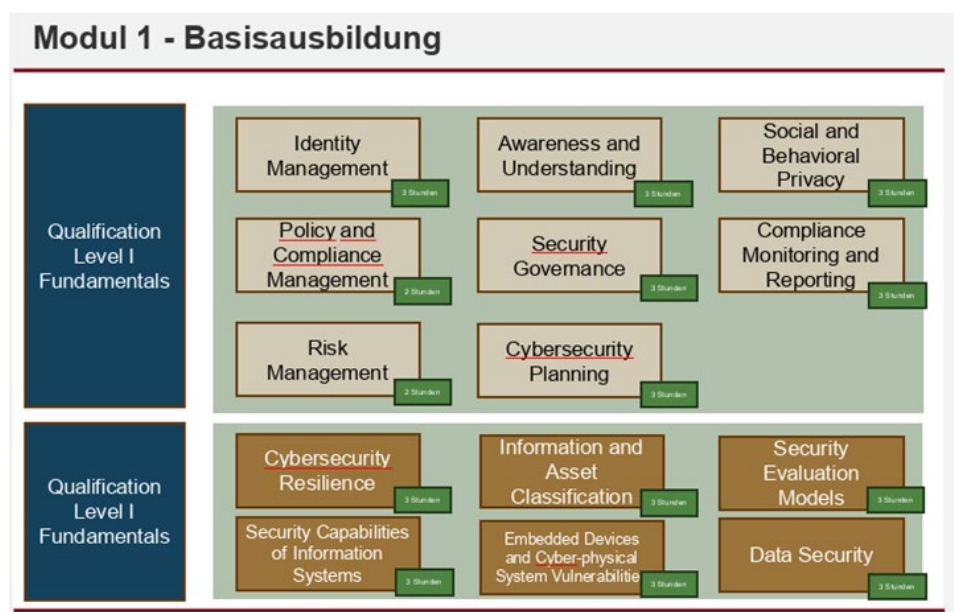


ABBILDUNG 32 CURRICULUM BASISAUSBILDUNG

Modul 2 – SOC

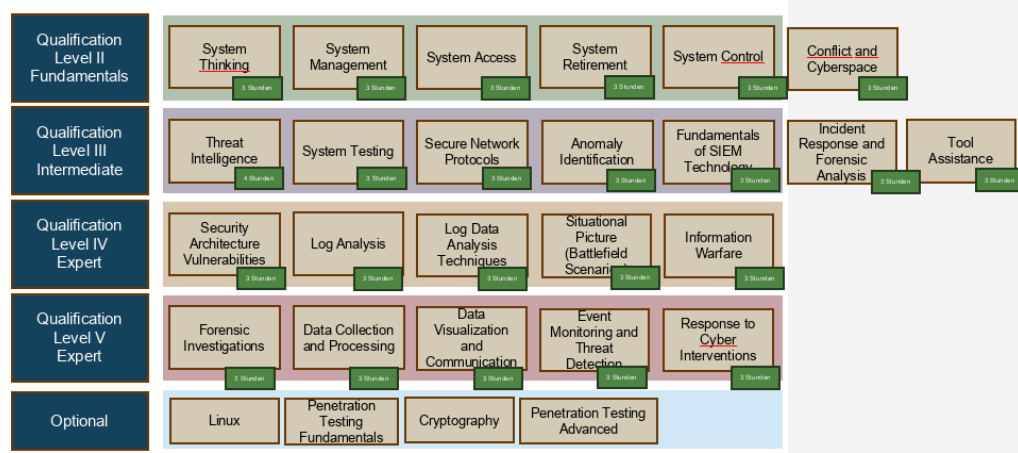


ABBILDUNG 33 CURRICULUM SOC MODUL 2

Modul 2 – NOC

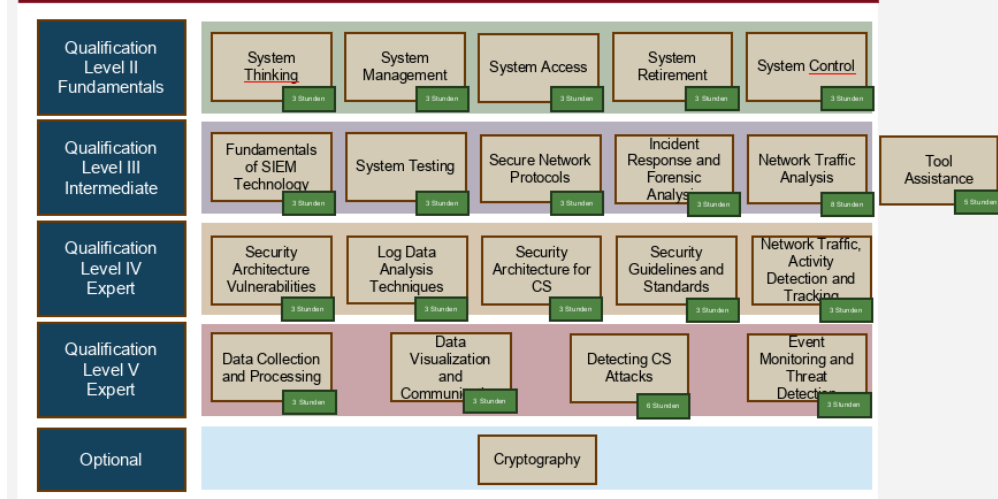


ABBILDUNG 34 CURRICULUM NOC MODUL 2

5.7.2.1 Identity Management

Das Wissensgebiet Identity Management behandelt die eindeutige Identifizierung, Authentisierung und Autorisierung von Personen, Diensten und Geräten im militärischen Umfeld. Es schafft die Grundlage dafür, Rollen sauber zu trennen, Zugriffe nach dem Need-to-know-Prinzip zu steuern und missbräuchliche oder kompromittierte Identitäten frühzeitig zu erkennen.

Vertieft behandelt werden dabei Lebenszyklus, Rezertifizierung und kontrollierte Deaktivierung von Benutzer-, Dienst- und Geräteidentitäten. Gerade im militärischen Umfeld entscheidet die saubere Trennung von Rollen, Zuständigkeiten und Privilegien darüber, ob sensible Informationen nur den tatsächlich berechtigten Stellen zugänglich bleiben.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 15 WISSENSEINHEITEN UND THEMEN IDENTITY MANAGEMENT

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Identitäts- und Rollenmodelle	Benutzeridentitäten, Dienstkonten, Geräteidentitäten, Rollen	Behandelt werden Aufbau, Zweck und Lebenszyklus unterschiedlicher Identitätstypen sowie ihre Zuordnung zu Aufgaben, Verantwortlichkeiten und Schutzbedarfen. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Authentisierung und Zugriffsschutz	MFA, Privilegien, Rezertifizierung, Protokollierung	Vermittelt werden Verfahren zur Absicherung privilegierter Zugriffe, zur regelmäßigen Überprüfung von Berechtigungen und zur Nachvollziehbarkeit sicherheitsrelevanter Anmeldungen. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Lebenszyklus und Nachweisführung	Provisionierung, Rezertifizierung, Offboarding, Audit Trails	Vertieft wird, wie Identity Management über den gesamten Lebenszyklus kontrolliert, regelmäßig überprüft und nachvollziehbar dokumentiert wird, um Berechtigungsreste, Missbrauch und Schattenstrukturen zu vermeiden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 16 KERNELEMENTE UND LERNERGEBNISSE IDENTITY MANAGEMENT

Kernelement	Lernergebnisse
Begriffs- und Rollenverständnis	Die Teilnehmenden unterscheiden Identifikation, Authentisierung und Autorisierung sicher und können diese Konzepte auf militärische IT- und Kommunikationssysteme anwenden. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Sichere Zugriffsgestaltung	Die Teilnehmenden leiten angemessene Maßnahmen für Rollenmodelle, Mehrfaktor-Authentisierung und den Schutz privilegierter Konten ab. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Identity Management auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

sichere Routinen im militärischen Alltag. Das Wissensgebiet verknüpft Cyber-Hygiene mit der Fähigkeit, verdächtige Anzeichen zu erkennen, korrekt zu melden und eigenes Verhalten an die Sicherheitslage anzupassen.

Das Wissensgebiet reicht deshalb über reine Sensibilisierungskampagnen hinaus und verbindet individuelles Verhalten mit Meldewegen, Führungsvorgaben und konkreten Schutzroutinen. Für den militärischen Alltag ist entscheidend, dass sich sicheres Verhalten auch unter Zeitdruck, in Übungs- und Einsatzlagen sowie bei eingeschränkter Informationslage verlässlich abrufen lässt.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsrountinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 17 WISSENSEINHEITEN UND THEMEN AWARENESS AND UNDERSTANDING

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Cyber-Hygiene	Passwörter, Endgeräte, Updates, sichere Nutzung	Im Mittelpunkt stehen alltägliche Schutzmaßnahmen, die das Risiko erfolgreicher Angriffe durch unbedachte Handlungen deutlich reduzieren. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Bedrohungsbewusstsein und Meldedisziplin	Phishing, Social Engineering, Warnsignale, Eskalation	Behandelt wird, wie verdächtige Vorkommnisse erkannt, eingeordnet und entlang definierter Meldewege an die zuständigen Stellen weitergegeben werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Verhaltenssteuerung und Kommunikation	SETA, Rollenbilder, Meldewege, Interventionen	Behandelt wird, wie Inhalte aus Awareness and Understanding in sicheres Verhalten, zielgruppengerechte Kommunikation und belastbare Melde- und Unterstützungswege überführt werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 18 KERNELEMENTE UND LERNERGEBNISSE AWARENESS AND UNDERSTANDING

Kernelement	Lernergebnisse
Gefahrenwahrnehmung	Die Teilnehmenden erkennen typische Angriffsindikatoren und können deren Relevanz für den eigenen Dienstbetrieb beurteilen.

	Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Sicheres Verhalten	Die Teilnehmenden wenden grundlegende Regeln sicherer Systemnutzung an und handeln bei Auffälligkeiten regelkonform und adressatengerecht. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Awareness and Understanding auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.2 Social and Behavioral Privacy

Dieses Wissensgebiet beleuchtet den Zusammenhang zwischen menschlichem Verhalten, Privatsphäre und operativer Sicherheit. Im Fokus stehen soziale Medien, Verhaltensmuster, Datenspuren und die Frage, wie scheinbar harmlose Informationen gegnerische Aufklärung, Profilbildung oder Einflussnahme unterstützen können.

Im Mittelpunkt stehen dabei Wechselwirkungen zwischen persönlicher Sichtbarkeit, sozialem Verhalten und operativer Sicherheit. Besonders in militärischen Kontexten können scheinbar harmlose Informationen über Routinen, Rollen, Standorte oder soziale Beziehungen zu Aufklärungs- und Einflusszwecken ausgenutzt werden.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 19 WISSENSEINHEITEN UND THEMEN SOCIAL AND BEHAVIORAL PRIVACY

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Privatsphäre in sozialen und digitalen Räumen	Social Media, Zielgruppen, Sichtbarkeit, Identitätsdarstellung	Vermittelt werden Risiken, die aus der Veröffentlichung, Verknüpfung und Fehlinterpretation persönlicher und dienstlicher Informationen entstehen. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Verhaltensbezogene Sicherheitsrisiken	Gewohnheiten, Routinen, Datenabgabe, Manipulation	Behandelt wird, wie Verhaltensmuster, Standortdaten oder Interaktionsprofile ausgenutzt werden können und wie dem präventiv begegnet wird. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Verhaltenssteuerung und Kommunikation	SETA, Rollenbilder, Meldewege, Interventionen	Behandelt wird, wie Inhalte aus Social and Behavioral Privacy in sicheres

		Verhalten, zielgruppengerechte Kommunikation und belastbare Melde- und Unterstützungswege überführt werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 20 KERNELEMENTE UND LERNERGEBNISSE SOCIAL AND BEHAVIORAL PRIVACY

Kernelement	Lernergebnisse
Privatsphäre als Sicherheitsfaktor	Die Teilnehmenden erklären, warum der Schutz persönlicher und dienstlicher Informationen ein operativ relevanter Bestandteil von Cyber-Sicherheit ist. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Risikobewusstes Verhalten	Die Teilnehmenden beurteilen soziale und verhaltensbezogene Datenschutzrisiken und passen ihre digitale Kommunikation entsprechend an. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Social and Behavioral Privacy auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.3 Policy and Compliance Management

Policy and Compliance Management behandelt die Übersetzung strategischer und rechtlicher Anforderungen in verbindliche Regeln, Verfahren und Kontrollmechanismen. Es schafft die Grundlage für einheitliches Handeln im Alltag, in Übungen und in besonderen Lagen und verbindet Richtlinienarbeit mit praktischer Umsetzbarkeit.

Vertieft wird insbesondere, wie Vorgaben nicht nur formuliert, sondern wirksam kommuniziert, in Prozesse übersetzt und im Alltag durchgesetzt werden. Für militärische Organisationen bedeutet dies, dass Richtlinien sowohl rechtssicher als auch unter Einsatz- und Übungsbedingungen praktisch anwendbar sein müssen.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 21 WISSENSEINHEITEN UND THEMEN POLICY AND COMPLIANCE MANAGEMENT

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Richtlinienentwicklung	Ziele, Verantwortlichkeiten, Verfahren, Ausnahmen	Die Teilnehmenden lernen, wie Sicherheitsrichtlinien adressatengerecht formuliert, abgestimmt und in Standardarbeitsanweisungen überführt werden. Dabei wird der

		Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Umsetzung und Nachverfolgung	Kommunikation, Schulung, Nachweise, Korrekturmaßnahmen	Behandelt wird, wie Vorgaben in den Betrieb eingebracht, deren Einhaltung überprüft und Abweichungen systematisch bearbeitet werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Steuerung, Nachweis und Verbesserung	Metriken, Reviews, Abweichungen, Reifegradentwicklung	Vermittelt wird, wie Policy and Compliance Management in überprüfbare Steuerungsmechanismen, Kennzahlen und kontinuierliche Verbesserungsprozesse übersetzt wird, damit Wirksamkeit und Nachvollziehbarkeit dauerhaft gesichert bleiben. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 22 KERNELEMENTE UND LERNERGEBNISSE POLICY AND COMPLIANCE MANAGEMENT

Kernelement	Lernergebnisse
Regelwerk und Praxisbezug	Die Teilnehmenden können Richtlinien und Compliance-Anforderungen in operative Prozesse und nachvollziehbare Verantwortlichkeiten übersetzen. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Steuerung von Abweichungen	Die Teilnehmenden erkennen Non-Compliance, leiten Korrekturmaßnahmen ab und dokumentieren deren Umsetzung nachvollziehbar. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Policy and Compliance Management auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.4 Security Governance

Security Governance beschreibt die Steuerung von Informations- und Cyber-Sicherheit als Führungsaufgabe. Das Wissensgebiet verknüpft Rollen, Zuständigkeiten, Entscheidungswege,

Prioritäten und Messgrößen und schafft so den organisatorischen Rahmen, in dem technische Maßnahmen sinnvoll geplant, freigegeben und bewertet werden.

Dazu gehört die Verknüpfung von Verantwortlichkeiten, Führungsstrukturen, Risikobewertung und Ressourcensteuerung. Sicherheitsgovernance schafft damit den Rahmen, innerhalb dessen technische Maßnahmen priorisiert, nachverfolgt und gegenüber Führungsebenen nachvollziehbar begründet werden können.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 23 WISSENSEINHEITEN UND THEMEN SECURITY GOVERNANCE

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Governance-Strukturen	Rollen, Zuständigkeiten, Gremien, Eskalation	Vermittelt werden Organisationsformen und Führungsbeziehungen, die für wirksame Sicherheitssteuerung im militärischen Umfeld erforderlich sind. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Steuerung und Messung	Kennzahlen, Zielbilder, Reifegrad, Berichtswesen	Behandelt wird, wie Sicherheitsziele operationalisiert, Fortschritte messbar gemacht und Führungsentscheidungen mit belastbaren Informationen unterlegt werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Steuerung, Nachweis und Verbesserung	Metriken, Reviews, Abweichungen, Reifegradentwicklung	Vermittelt wird, wie Security Governance in überprüfbare Steuerungsmechanismen, Kennzahlen und kontinuierliche Verbesserungsprozesse übersetzt wird, damit Wirksamkeit und Nachvollziehbarkeit dauerhaft gesichert bleiben. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 24 KERNELEMENTE UND LERNERGEBNISSE SECURITY GOVERNANCE

Kernelement	Lernergebnisse

Führungs- und Steuerungsverständnis	Die Teilnehmenden erklären, wie Security Governance technische, organisatorische und operative Perspektiven zusammenführt. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Entscheidungsunterstützung	Die Teilnehmenden nutzen Kennzahlen und Rollenmodelle, um Sicherheitsmaßnahmen nachvollziehbar zu priorisieren und zu steuern. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Security Governance auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.5 Compliance Monitoring and Reporting

Dieses Wissensgebiet fokussiert die laufende Überwachung regulatorischer, organisatorischer und interner Anforderungen sowie die adressatengerechte Berichterstattung. Es unterstützt eine belastbare Nachweisführung und schafft Transparenz darüber, wo Vorgaben erfüllt, wo Risiken erhöht und wo Gegenmaßnahmen erforderlich sind.

Besonderes Gewicht liegt auf der Fähigkeit, Anforderungen dauerhaft nachweisbar einzuhalten und Abweichungen früh zu erkennen. Im militärischen Kontext müssen Monitoring und Reporting so gestaltet werden, dass sie Prüf- und Führungsbedarfe erfüllen, ohne den laufenden Betrieb unnötig zu belasten.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 25 WISSENSEINHEITEN UND THEMEN COMPLIANCE MONITORING AND REPORTING

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Monitoring von Anforderungen	Kontrollen, Audits, Evidenzen, Prüfpfade	Behandelt werden Verfahren, mit denen die Einhaltung relevanter Vorgaben kontinuierlich beobachtet und dokumentiert wird. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Berichtswesen und Kommunikation	Compliance-Reports, Management-Sichten, Eskalation	Vermittelt wird, wie Ergebnisse verdichtet, bewertet und für unterschiedliche Entscheidungsebenen verständlich dargestellt werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

Steuerung, Nachweis und Verbesserung	Metriken, Reviews, Abweichungen, Reifegradentwicklung	Vermittelt wird, wie Compliance Monitoring and Reporting in überprüfbare Steuerungsmechanismen, Kennzahlen und kontinuierliche Verbesserungsprozesse übersetzt wird, damit Wirksamkeit und Nachvollziehbarkeit dauerhaft gesichert bleiben. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 26 KERNELEMENTE UND LERNERGEBNISSE COMPLIANCE MONITORING AND REPORTING

Kernelement	Lernergebnisse
Nachweisfähigkeit	Die Teilnehmenden richten Überwachungs- und Nachweisverfahren ein, mit denen Compliance-Aussagen belastbar belegt werden können. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Adressatengerechtes Reporting	Die Teilnehmenden erstellen Berichte, die Abweichungen, Risiken und Handlungsbedarf klar und nachvollziehbar kommunizieren. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Compliance Monitoring and Reporting auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.6 Risk Management

Risk Management befasst sich mit der systematischen Identifikation, Bewertung, Behandlung und Kommunikation von Risiken für Informationen, Systeme und Missionen. Das Wissensgebiet stellt sicher, dass Bedrohungen und Verwundbarkeiten nicht isoliert betrachtet, sondern im Hinblick auf operative Wirkung, Priorisierung und Restrestisiko bewertet werden.

Dazu werden Risiken nicht isoliert betrachtet, sondern in ihren Auswirkungen auf Auftragserfüllung, Einsatzbereitschaft und Interoperabilität eingeordnet. Entscheidend ist die Fähigkeit, technische, organisatorische und operationelle Risiken in einem gemeinsamen Bewertungsrahmen zusammenzuführen.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsrouniten entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 27 WISSENSEINHEITEN UND THEMEN RISK MANAGEMENT

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Risikoidentifikation und -analyse	Assets, Bedrohungen, Schwachstellen, Auswirkungen	Im Fokus stehen Methoden, um Risiken zu erfassen, zu strukturieren und hinsichtlich Eintrittswahrscheinlichkeit und Schadenspotenzial zu bewerten. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Risikobehandlung	Vermeiden, Reduzieren, Übertragen, Akzeptieren	Behandelt wird, wie Maßnahmen ausgewählt, Restrestrisiken kommuniziert und Entscheidungen entlang von Führungs- und Freigabeketten vorbereitet werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Steuerung, Nachweis und Verbesserung	Metriken, Reviews, Abweichungen, Reifegradentwicklung	Vermittelt wird, wie Risk Management in überprüfbare Steuerungsmechanismen, Kennzahlen und kontinuierliche Verbesserungsprozesse übersetzt wird, damit Wirksamkeit und Nachvollziehbarkeit dauerhaft gesichert bleiben. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 28 KERNELEMENTE UND LERNERGEBNISSE RISK MANAGEMENT

Kernelement	Lernergebnisse
Risikoorientiertes Denken	Die Teilnehmenden führen strukturierte Risikoabschätzungen durch und priorisieren Risiken nach Schutzbedarf und Missionsbezug. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Entscheidungsreife Maßnahmen	Die Teilnehmenden leiten geeignete Behandlungsoptionen ab und kommunizieren verbleibende Risiken transparent an Entscheidungsträger. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Risk Management auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.7 Cybersecurity Planning

Cybersecurity Planning behandelt die Übersetzung von Sicherheitszielen in umsetzbare Planungen auf strategischer, operativer und taktischer Ebene. Das Wissensgebiet verbindet Lagebild, Ressourcen, Abhängigkeiten und Zeitplanung und schafft damit eine belastbare Grundlage für Schutz-, Erkennungs- und Reaktionsmaßnahmen.

Die Planungsperspektive umfasst strategische Zielbilder ebenso wie umsetzbare Roadmaps, Prioritäten und Abhängigkeiten. Für das Bumblebee-Curriculum ist wichtig, dass Planungsentscheidungen stets an Auftrag, Kritikalität, vorhandenen Ressourcen und realistischen Umsetzungswegen ausgerichtet werden.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 29 WISSENSEINHEITEN UND THEMEN CYBERSECURITY PLANNING

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Strategische Planung	Zielbild, Prioritäten, Ressourcen, Roadmap	Vermittelt wird, wie Sicherheitsvorhaben aus Auftrag, Bedrohung und Reifegrad abgeleitet und in mittelfristige Entwicklungspfade übersetzt werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Operative Planungsprodukte	Playbooks, Zuständigkeiten, Kommunikationswege, Übungen	Behandelt wird die Erstellung konkreter Planungsprodukte, die im Betrieb und in besonderen Lagen handlungsleitend wirken. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Steuerung, Nachweis und Verbesserung	Metriken, Reviews, Abweichungen, Reifegradentwicklung	Vermittelt wird, wie Cybersecurity Planning in überprüfbare Steuerungsmechanismen, Kennzahlen und kontinuierliche Verbesserungsprozesse übersetzt wird, damit Wirksamkeit und Nachvollziehbarkeit dauerhaft gesichert bleiben. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 30 KERNELEMENTE UND LERNERGEBNISSE CYBERSECURITY PLANNING

Kernelement	Lernergebnisse
Planungsfähigkeit	Die Teilnehmenden entwickeln strukturierte Cyber-Sicherheitspläne, die Ziele, Ressourcen und Verantwortlichkeiten konsistent zusammenführen. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Umsetzungsbezug	Die Teilnehmenden überführen strategische Vorgaben in operative Maßnahmenpakete und nachvollziehbare Handlungsanweisungen. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Cybersecurity Planning auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.8 Cybersecurity Resilience

Cybersecurity Resilience fokussiert die Fähigkeit, trotz Störungen und Angriffen handlungsfähig zu bleiben, Funktionen kontrolliert zu degradieren und zentrale Fähigkeiten rasch wiederherzustellen. Im Zentrum stehen Robustheit, Wiederanlauf, Ausweichverfahren und das bewusste Management von Betriebsfähigkeit unter Belastung.

Resilienz bedeutet hier mehr als Wiederherstellung nach einem Vorfall; sie umfasst Vorsorge, robuste Betriebsführung, degradierte Betriebsarten und lernfähige Verbesserungsprozesse. Im militärischen Umfeld muss Resilienz auch dann wirken, wenn Teile von Infrastruktur, Kommunikation oder Unterstützung nur eingeschränkt verfügbar sind.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsrouniten entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 31 WISSENSEINHEITEN UND THEMEN CYBERSECURITY RESILIENCE

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Resilienzprinzipien	Redundanz, Segmentierung, Notbetrieb, Priorisierung	Vermittelt werden Gestaltungsprinzipien, mit denen Systeme und Prozesse widerstandsfähiger gegenüber technischen und gegnerischen Einwirkungen werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Wiederherstellung und Continuity	Recovery, Wiederanlaufpläne, Übungen, Lessons Learned	Behandelt wird, wie Wiederherstellung vorbereitet, getestet und auf Basis von Erfahrungen schrittweise verbessert

		wird. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Schutzmaßnahmen über den Lebenszyklus	Vorsorge, Härtung, Wiederherstellung, Integritätssicherung	Behandelt wird, wie Maßnahmen aus Cybersecurity Resilience entlang des gesamten Lebenszyklus von Daten, Prozessen oder Diensten geplant, umgesetzt und regelmäßig überprüft werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 32 KERNELEMENTE UND LERNERGEBNISSE CYBERSECURITY RESILIENCE

Kernelement	Lernergebnisse
Fight-through-Fähigkeit	Die Teilnehmenden erklären, wie wesentliche Dienste unter Angriff oder Störung aufrechterhalten und kontrolliert priorisiert werden können. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Wiederherstellungsplanung	Die Teilnehmenden entwerfen Wiederanlauf- und Ausweichverfahren, die technische und operative Abhängigkeiten berücksichtigen. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Cybersecurity Resilience auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.9 Information and Asset Classification

Dieses Wissensgebiet behandelt die strukturierte Erfassung und Klassifikation von Informationen, Diensten, Systemen und Komponenten. Es schafft die Grundlage für Schutzbedarf, Freigaben, Zugriffsrechte und technische Schutzmaßnahmen und unterstützt eine konsistente Priorisierung im Betrieb und in Krisensituationen.

Die Klassifikation schafft die Voraussetzung dafür, Schutzbedarf, Zugriffsrechte und Handhabungsvorschriften konsistent zu begründen. Sie ist besonders relevant, wenn Informationen, Systeme und Datenflüsse organisationsübergreifend genutzt oder in abgestuften Führungs- und Einsatzkontexten verarbeitet werden.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 33 WISSENSEINHEITEN UND THEMEN INFORMATION AND ASSET CLASSIFICATION

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Asset-Inventarisierung und Kritikalität	Asset-Kataloge, Abhängigkeiten, Kritikalität, Verantwortliche	Behandelt werden Verfahren zur vollständigen und nachvollziehbaren Erfassung sicherheitsrelevanter Güter und ihrer Abhängigkeiten. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Klassifikation und Handhabung	Schutzbedarf, Einstufung, Kennzeichnung, Weitergabe	Vermittelt werden Regeln und Prozesse zur angemessenen Klassifikation sowie zur sicheren Verarbeitung und Weitergabe von Informationen. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Schutzmaßnahmen über den Lebenszyklus	Vorsorge, Härtung, Wiederherstellung, Integritätssicherung	Behandelt wird, wie Maßnahmen aus Information and Asset Classification entlang des gesamten Lebenszyklus von Daten, Prozessen oder Diensten geplant, umgesetzt und regelmäßig überprüft werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 34 KERNELEMENTE UND LERNERGEBNISSE INFORMATION AND ASSET CLASSIFICATION

Kernelement	Lernergebnisse
Strukturierter Überblick	Die Teilnehmenden erstellen nachvollziehbare Asset- und Informationsklassifikationen als Grundlage für Schutzmaßnahmen und Priorisierung. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Schutzbedarfsgerechte Handhabung	Die Teilnehmenden wenden Klassifikationsregeln sicher an und berücksichtigen diese in Betrieb, Analyse und Meldung. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Information and Asset Classification auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.10 Security Evaluation Models

Security Evaluation Models befassen sich mit Kriterien und Modellen zur Bewertung von Sicherheitsmaßnahmen, Architekturen und Reifegraden. Das Wissensgebiet unterstützt eine vergleichbare und nachvollziehbare Beurteilung, welche Kontrollen wirksam sind, welche Lücken bestehen und wo Investitionen oder Anpassungen prioritär sind.

Behandelt wird außerdem, wie Reifegrade, Bewertungsmodelle und Prüfmaßstäbe dazu beitragen, Sicherheitslagen vergleichbar und entwickelbar zu machen. Solche Modelle unterstützen Führung und Fachpersonal dabei, Prioritäten zu setzen und Fortschritte belastbar nachzuweisen.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 35 WISSENSEINHEITEN UND THEMEN SECURITY EVALUATION MODELS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Bewertungsmodelle und Kriterien	Reifegrade, Scorecards, Wirksamkeit, Vergleichbarkeit	Vermittelt werden Verfahren, mit denen Sicherheitslage und Kontrollqualität methodisch bewertet und über die Zeit beobachtet werden können. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Entscheidungsunterstützung	Trade-offs, Priorisierung, Soll-Ist-Abgleich, Verbesserungen	Behandelt wird, wie Bewertungsergebnisse in Maßnahmenplanung, Ressourcensteuerung und Architekturentscheidungen einfließen. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Steuerung, Nachweis und Verbesserung	Metriken, Reviews, Abweichungen, Reifegradentwicklung	Vermittelt wird, wie Security Evaluation Models in überprüfbare Steuerungsmechanismen, Kennzahlen und kontinuierliche Verbesserungsprozesse übersetzt wird, damit Wirksamkeit und Nachvollziehbarkeit dauerhaft gesichert bleiben. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 36 KERNELEMENTE UND LERNERGEBNISSE SECURITY EVALUATION MODELS

Kernelement	Lernergebnisse
Methodische Bewertung	Die Teilnehmenden wählen geeignete Bewertungsmodelle aus und wenden sie auf Sicherheitskontrollen, Architekturen und Prozesse an. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Ableitung von Verbesserungen	Die Teilnehmenden interpretieren Bewertungsergebnisse und übersetzen diese in priorisierte Verbesserungsmaßnahmen. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Security Evaluation Models auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.11 Security Capabilities of Information Systems

Dieses Wissensgebiet behandelt die sicherheitsrelevanten Fähigkeiten moderner Informationssysteme selbst. Dazu zählen eingebaute Schutzmechanismen, Härtungsoptionen, Protokollierungsfunktionen, Schnittstellenkontrollen und Möglichkeiten zur sicheren Integration in größere Systemverbünde.

Im Fokus steht die Frage, welche Sicherheitsfähigkeiten Informationssysteme von sich aus bereitstellen und wo ergänzende Maßnahmen erforderlich werden. Damit wird eine Grundlage geschaffen, um Systeme nicht nur nach Funktionalität, sondern auch nach ihrem Beitrag zu Schutz, Detektion und Nachvollziehbarkeit zu bewerten.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsrouniten entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 37 WISSENSEINHEITEN UND THEMEN SECURITY CAPABILITIES OF INFORMATION SYSTEMS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Integrierte Sicherheitsfunktionen	Härtung, Logging, Rechteverwaltung, Schutzmechanismen	Die Teilnehmenden lernen, welche systemseitigen Fähigkeiten zur Sicherung von Vertraulichkeit, Integrität und Verfügbarkeit genutzt werden können. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Sichere Integration	Schnittstellen, Interoperabilität, Abhängigkeiten, Baselines	Behandelt wird, wie Sicherheitsfunktionen in heterogenen Umgebungen konsistent eingesetzt und in sichere Baselines überführt

		werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie Security Capabilities of Information Systems an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 38 KERNELEMENTE UND LERNERGEBNISSE SECURITY CAPABILITIES OF INFORMATION SYSTEMS

Kernelement	Lernergebnisse
Systemimmanente Sicherheit	Die Teilnehmenden beurteilen, welche Schutzfunktionen ein Informationssystem nativ bereitstellt und wie diese wirksam genutzt werden. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Technische Umsetzbarkeit	Die Teilnehmenden integrieren Sicherheitsfähigkeiten in Baselines und Hardening-Maßnahmen für den realen Betrieb. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Security Capabilities of Information Systems auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.12 *Embedded Devices and Cyber-physical System Vulnerability*

Das Wissensgebiet adressiert die besonderen Verwundbarkeiten eingebetteter Systeme sowie cyber-physischer Komponenten. Es verbindet Architekturverständnis mit der Analyse von Angriffsflächen, Auswirkungen auf physische Prozesse und den Grenzen klassischer IT-Sicherheitsmaßnahmen in OT-nahen Umgebungen.

Das Wissensgebiet berücksichtigt insbesondere die Besonderheiten eingebetteter und cyber-physischer Systeme wie begrenzte Ressourcen, lange Lebenszyklen und enge Kopplungen an physische Prozesse. Sicherheitsprobleme können hier unmittelbare Auswirkungen auf Verfügbarkeit, Safety und Missionsfähigkeit haben.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsroutinen entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische

Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 39 WISSENSEINHEITEN UND THEMEN EMBEDDED DEVICES AND CYBER-PHYSICAL SYSTEM VULNERABILITY

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Architekturen eingebetteter und cyber-physischer Systeme	Firmware, Sensorik, Aktorik, Echtzeit, Schnittstellen	Vermittelt wird, wie sich technische Besonderheiten solcher Systeme auf Schutzbedarf, Beobachtbarkeit und Härbarkeit auswirken. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Verwundbarkeiten und Auswirkungen	Unsichere Protokolle, physische Effekte, Patchgrenzen, Kompensation	Behandelt werden typische Schwachstellen sowie Möglichkeiten zur Risikoabschwächung, wenn direkte Änderungen an Systemen nur eingeschränkt möglich sind. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie Embedded Devices and Cyber-physical System Vulnerability an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 40 KERNELEMENTE UND LERNERGEBNISSE EMBEDDED DEVICES AND CYBER-PHYSICAL SYSTEM VULNERABILITY

Kernelement	Lernergebnisse
Spezifisches OT-/Embedded-Verständnis	Die Teilnehmenden erkennen Unterschiede zwischen klassischen IT-Systemen und eingebetteten bzw. cyber-physischen Komponenten. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Risikomindernde Maßnahmen	Die Teilnehmenden leiten kompensierende Schutzmaßnahmen für schwer patchbare oder betriebsnahe Systeme ab. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Embedded Devices and Cyber-physical System Vulnerability auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei

	angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.2.13 Data Security

Data Security behandelt den Schutz von Daten über ihren gesamten Lebenszyklus hinweg – von Erzeugung und Speicherung über Übertragung und Nutzung bis hin zu Archivierung und Löschung. Das Wissensgebiet verknüpft technische Kontrollen mit organisatorischen Regeln zur sicheren Datenverarbeitung.

Im Zentrum stehen Schutzmaßnahmen für Daten über ihren gesamten Lebenszyklus hinweg, von der Erhebung über Verarbeitung und Speicherung bis zur Weitergabe und Löschung. Militärische Szenarien verlangen dabei eine besonders sorgfältige Betrachtung von Vertraulichkeit, Integrität, Herkunft und Nachvollziehbarkeit.

In der Basisausbildung wird das Wissensgebiet deshalb so vermittelt, dass ein gemeinsames fachliches Vokabular, ein belastbares Sicherheitsverständnis und erste anwendungsnahe Handlungsrouniten entstehen. Die Teilnehmenden sollen zentrale Konzepte erklären, typische Risiken erkennen und einfache Maßnahmen in ihrem jeweiligen Verantwortungsbereich begründet anwenden können.

TABELLE 41 WISSENSEINHEITEN UND THEMEN DATA SECURITY

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Schutz des Datenlebenszyklus	Speicherung, Transport, Nutzung, Archivierung, Löschung	Vermittelt werden Bedrohungen und Schutzmaßnahmen entlang aller Phasen, in denen Daten erstellt, verändert, übertragen oder aufbewahrt werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Kontrollmechanismen	Verschlüsselung, Backups, DLP, Zugriffsregeln, Integrität	Behandelt werden technische und organisatorische Maßnahmen zur Verhinderung von Datenabfluss, Manipulation und unzulässiger Offenlegung. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und technischen Schutzmaßnahmen ausdrücklich mit betrachtet.
Schutzmaßnahmen über den Lebenszyklus	Vorsorge, Härtung, Wiederherstellung, Integritätssicherung	Behandelt wird, wie Maßnahmen aus Data Security entlang des gesamten Lebenszyklus von Daten, Prozessen oder Diensten geplant, umgesetzt und regelmäßig überprüft werden. Dabei wird der Zusammenhang zwischen individuellem Handeln, organisatorischen Vorgaben und

		technischen Schutzmaßnahmen ausdrücklich mit betrachtet.

TABELLE 42 KERNELEMENTE UND LERNERGEBNISSE DATA SECURITY

Kernelement	Lernergebnisse
Lebenszyklusorientierter Schutz	Die Teilnehmenden planen angemessene Schutzmaßnahmen für Daten in unterschiedlichen Verarbeitungs- und Einsatzkontexten. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Integrität und Verfügbarkeit	Die Teilnehmenden kombinieren Vertraulichkeits-, Integritäts- und Verfügbarkeitsmaßnahmen zu einem konsistenten Datensicherheitskonzept. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.
Operative Anschlussfähigkeit	Die Teilnehmenden übertragen Konzepte aus Data Security auf typische Situationen aus Dienstbetrieb, Übung und Einsatz und wählen dabei angemessene Schutz-, Melde- oder Unterstützungsmaßnahmen aus. Sie begründen ihr Vorgehen im Hinblick auf Schutzbedarf, Zuständigkeiten und typische Fehlerszenarien.

5.7.3 Gemeinsame operationelle Knowledge Areas von SOC und NOC

Die folgenden Wissensgebiete bilden das gemeinsame operationelle Fundament von SOC und NOC. Sie verbinden Systemverständnis, Überwachung, Analyse, Reaktion und technische Steuerung und schaffen damit eine gemeinsame Sprache für den Schicht- und Einsatzbetrieb.

TABELLE 43 GEMEINSAME KNOWLEDGE AREAS

Knowledge Area	Typische Verortung
System Thinking	SOC/NOC – Fundament
System Management	SOC/NOC – Fundament
System Access	SOC/NOC – Fundament
System Retirement	SOC/NOC – Fundament
System Control	SOC/NOC – Fundament
System Testing	SOC/NOC – Intermediate
Secure Network Protocols	SOC/NOC – Intermediate
Fundamentals of SIEM Technology	SOC/NOC – Intermediate
Incident Response and Forensic Analysis	SOC/NOC – Intermediate
Tool Assistance	SOC/NOC – Intermediate
Security Architecture Vulnerabilities	SOC/NOC – Expert
Log Data Analysis Techniques	SOC/NOC – Expert
Data Collection and Processing	SOC/NOC – Expert
Data Visualization and Communication	SOC/NOC – Expert
Event Monitoring and Threat Detection	SOC/NOC – Expert
Cryptography	Optional / gemeinsame Vertiefung

5.7.3.1 System Thinking

System Thinking vermittelt die Fähigkeit, Systeme nicht als lose Sammlung von Komponenten, sondern als funktional verbundenes Ganzes zu betrachten. Für SOC und NOC ist dieses Verständnis wesentlich, um Abhängigkeiten, Seiteneffekte und operative Konsequenzen technischer Maßnahmen richtig einzuordnen.

System Thinking erweitert den Blick von einzelnen Komponenten auf Abhängigkeiten, Wechselwirkungen und emergente Risiken in komplexen Verbünden. Für SOC und NOC ist dieses Denken zentral, weil Störungen und Angriffe selten an technischen Systemgrenzen Halt machen.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 44 WISSENSEINHEITEN UND THEMEN SYSTEM THINKING

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Systemgrenzen und Kontext	Umgebung, Schnittstellen, Abhängigkeiten, Wirkung	Behandelt wird, wie Systeme durch ihre Beziehungen zur Umgebung geprägt werden und warum Kontext für jede Sicherheitsbewertung mitgedacht werden muss. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Ganzheitliche Lagebeurteilung	Kaskadeneffekte, Nebenwirkungen, Prioritäten	Vermittelt werden Methoden, um technische Änderungen oder Störungen im Hinblick auf den Gesamtbetrieb und den Auftrag zu bewerten. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie System Thinking an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 45 KERNELEMENTE UND LERNERGEBNISSE SYSTEM THINKING

Kernelement	Lernergebnisse
Ganzheitliches Verständnis	Die Teilnehmenden analysieren Systeme unter Berücksichtigung von Abhängigkeiten, Schnittstellen und operativer Wirkung. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

Folgenabschätzung	Die Teilnehmenden leiten aus Störungen und Maßnahmen mögliche Seiteneffekte auf andere Dienste und Missionen ab. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen System Thinking so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.2 System Management

System Management behandelt den sicheren Betrieb und die kontrollierte Verwaltung von Systemen über ihren Lebenszyklus. Im Fokus stehen Konfiguration, Änderungsmanagement, Baselines, Nachvollziehbarkeit und die Integration sicherheitsrelevanter Aspekte in Routine- und Sonderprozesse.

Das Wissensgebiet behandelt daher nicht nur technische Administration, sondern auch Konfigurationskontrolle, Änderungsmanagement, Verantwortlichkeiten und betriebliche Nachweisführung. Gute Systemführung schafft die Voraussetzung dafür, Sicherheitsmaßnahmen konsistent und reproduzierbar umzusetzen.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 46 WISSENSEINHEITEN UND THEMEN SYSTEM MANAGEMENT

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Sicherer Betrieb	Baselines, Konfigurationsmanagement, Hardening, Dokumentation	Vermittelt werden Prinzipien, mit denen Systeme konsistent, nachvollziehbar und kontrollierbar betrieben werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Änderungs- und Freigabeprozesse	Change Management, Freigaben, Rollback, Risiken	Behandelt wird, wie Änderungen sicher vorbereitet, getestet, dokumentiert und bei Bedarf wieder zurückgeführt werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie System Management an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich

		sind. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 47 KERNELEMENTE UND LERNERGEBNISSE SYSTEM MANAGEMENT

Kernelement	Lernergebnisse
Betriebsdisziplin	Die Teilnehmenden halten sichere Betriebs- und Konfigurationsgrundsätze ein und erkennen risikoreiche Abweichungen. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Kontrollierte Änderungen	Die Teilnehmenden planen Änderungen so, dass Sicherheit, Verfügbarkeit und Nachvollziehbarkeit gemeinsam berücksichtigt werden. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen System Management so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.3 System Access

System Access fokussiert die sichere Anbindung von Menschen und Systemen an geschützte Umgebungen. Das Wissensgebiet behandelt Authentisierungsmethoden, Zugangswege, Vertrauensannahmen und die Absicherung menschlicher wie maschineller Interaktionen im Betrieb.

Besonders relevant ist die kontrollierte Vergabe, Nutzung und Überwachung von Zugriffen auf Systeme, Schnittstellen und Administrationsfunktionen. Fehlerhafte oder unzureichend gesteuerte Zugänge gehören zu den häufigsten Ursachen für Sicherheitsvorfälle und Folgekompromittierungen.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 48 WISSENSEINHEITEN UND THEMEN SYSTEM ACCESS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Zugriffswege und Authentisierung	Passwörter, Token, Zertifikate, SSO, MFA	Vermittelt werden die Eigenschaften unterschiedlicher Zugriffsverfahren sowie ihre Eignung für verschiedene Einsatz- und Bedrohungslagen. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb,

		Monitoring, Eskalation und nachvollziehbare Dokumentation.
Absicherung von Zugriffspfaden	Remote Access, Administrationszugänge, Vertrauensgrenzen	Behandelt wird, wie Zugangswege überwacht, eingeschränkt und gegen Missbrauch abgesichert werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Lebenszyklus und Nachweisführung	Provisionierung, Rezertifizierung, Offboarding, Audit Trails	Vertieft wird, wie System Access über den gesamten Lebenszyklus kontrolliert, regelmäßig überprüft und nachvollziehbar dokumentiert wird, um Berechtigungsreste, Missbrauch und Schattenstrukturen zu vermeiden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 49 KERNELEMENTE UND LERNERGEBNISSE SYSTEM ACCESS

Kernelement	Lernergebnisse
Methodenverständnis	Die Teilnehmenden vergleichen Authentisierungsverfahren hinsichtlich Sicherheit, Handhabbarkeit und Missionsbezug. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Sichere Zugriffspfade	Die Teilnehmenden gestalten Zugriffswege so, dass unbefugter Zugriff erschwert und privilegierte Nutzung kontrollierbar bleibt. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen System Access so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.4 System Retirement

System Retirement behandelt die sichere Außerbetriebnahme, Migration oder Stilllegung von Systemen und Komponenten. Gerade in militärischen Umgebungen ist entscheidend, dass Restdaten, Altverbindungen, implizite Abhängigkeiten und Folgeeffekte frühzeitig erkannt und kontrolliert werden.

Die sichere Außerbetriebnahme von Systemen ist ein oft unterschätzter Teil des Sicherheitslebenszyklus. Gerade Alt- und Übergangssysteme erzeugen Risiken durch Datenreste, vergessene Zugänge, verbleibende Abhängigkeiten oder unvollständig dokumentierte Schnittstellen.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit

benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 50 WISSENSEINHEITEN UND THEMEN SYSTEM RETIREMENT

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Planung der Außerbetriebnahme	Abhängigkeiten, Datenübernahme, Parallelbetrieb, Risiken	Die Teilnehmenden lernen, welche technischen und organisatorischen Aspekte vor der Stilllegung eines Systems berücksichtigt werden müssen. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Sichere Stilllegung	Datenbereinigung, Abschaltung, Entsorgung, Nachweisführung	Behandelt werden Verfahren zur sicheren Entfernung von Restzugängen, Datenbeständen und Konfigurationsartefakten. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie System Retirement an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 51 KERNELEMENTE UND LERNERGEBNISSE SYSTEM RETIREMENT

Kernelement	Lernergebnisse
Risikobewusste Stilllegung	Die Teilnehmenden identifizieren sicherheitsrelevante Auswirkungen von Decommissioning-Vorhaben auf den Gesamtbetrieb. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Saubere Übergänge	Die Teilnehmenden planen und dokumentieren Außerbetriebnahmen so, dass Sicherheitslücken und Betriebsunterbrechungen minimiert werden. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen System Retirement so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.5 System Control

System Control behandelt Steuerungs- und Kontrollmechanismen, mit denen Systemverhalten beeinflusst, Zugriffe durchgesetzt und Sicherheitszustände überwacht werden. Dazu gehören Autorisierung, Richtlinienumsetzung sowie technische Kontrollen zur Durchsetzung definierter Sicherheitsziele.

Kontrolle umfasst hier die Fähigkeit, Systemzustände zu beobachten, Konfigurationen durchzusetzen und ungewollte Veränderungen rechtzeitig sichtbar zu machen. Sie verbindet technische Steuerbarkeit mit Nachvollziehbarkeit und operativer Entscheidungsfähigkeit.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 52 WISSENSEINHEITEN UND THEMEN SYSTEM CONTROL

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Autorisierung und Steuerungsmodelle	RBAC, MAC, DAC, Regelwerke, Durchsetzung	Vermittelt werden Zugriffskonzepte und Mechanismen, mit denen Systemverhalten regelgeleitet und überprüfbar gesteuert wird. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Kontrolle und Nachvollziehbarkeit	Audit, Durchsetzung, Sperren, Protokollierung	Behandelt wird, wie Kontrollmechanismen sichtbar, überprüfbar und gegenüber Missbrauch widerstandsfähig gemacht werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie System Control an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 53 KERNELEMENTE UND LERNERGEBNISSE SYSTEM CONTROL

Kernelement	Lernergebnisse
Kontrolllogik	Die Teilnehmenden erklären, wie Steuerungs- und Autorisierungsmechanismen zusammenwirken, um sichere Betriebszustände zu unterstützen. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

Durchsetzung sicherer Zustände	Die Teilnehmenden wählen geeignete Kontrollmechanismen aus, um Risiken zu begrenzen und Regeln technisch umzusetzen. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen System Control so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.6 System Testing

System Testing fokussiert die Überprüfung, ob Systeme, Komponenten und Konfigurationen ihre Sicherheitsanforderungen tatsächlich erfüllen. Dazu gehören technische Tests, Funktionsprüfungen, Integrationsprüfungen und die strukturierte Bewertung von Befunden im Hinblick auf den realen Betrieb.

Getestet wird nicht nur, ob Anforderungen formal erfüllt sind, sondern ob Schutzmaßnahmen unter realistischen Betriebsbedingungen tatsächlich wirksam bleiben. Dies schließt Validierung, Fehlersuche, Schwachstellenprüfung und die Bewertung von Nebenwirkungen geplanter Änderungen ein.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 54 WISSENSEINHEITEN UND THEMEN SYSTEM TESTING

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Sicherheitsbezogene Testverfahren	Vulnerability Scans, Penetration Tests, Konfigurationsprüfungen	Behandelt werden Testformen, mit denen Schwachstellen, Fehlkonfigurationen und unerwartetes Verhalten sichtbar gemacht werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Validierung von Anforderungen	Soll-Ist-Abgleich, Testfälle, Akzeptanzkriterien, Nachtests	Vermittelt wird, wie Testaktivitäten auf Sicherheitsziele bezogen, Ergebnisse dokumentiert und Korrekturen abgesichert werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie System Testing an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Besonderes Gewicht liegt auf der

		Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 55 KERNELEMENTE UND LERNERGEBNISSE SYSTEM TESTING

Kernelement	Lernergebnisse
Prüfbarkeit	Die Teilnehmenden leiten geeignete Testverfahren aus Sicherheitsanforderungen ab und interpretieren die Ergebnisse fachgerecht. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Verbesserungsorientierung	Die Teilnehmenden priorisieren Befunde und planen Nachtests, um die Wirksamkeit umgesetzter Maßnahmen zu verifizieren. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen System Testing so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.7 Secure Network Protocols

Secure Network Protocols behandelt Protokolle und Kommunikationsmechanismen, die für den sicheren Datenaustausch in Netzen und Systemverbünden erforderlich sind. Das Wissensgebiet verbindet Protokollverständnis mit Härtung, Fehlkonfigurationsrisiken und der Auswahl angemessener Schutzmechanismen.

Das Wissensgebiet betrachtet Protokolle nicht als neutrale Transportmechanismen, sondern als sicherheitsrelevante Entwurfs- und Betriebsentscheidungen. Authentisierung, Integritätsschutz, Schlüsselaustausch und Fehlkonfigurationen wirken sich unmittelbar auf Vertraulichkeit, Stabilität und Überwachbarkeit aus.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 56 WISSENSEINHEITEN UND THEMEN SECURE NETWORK PROTOCOLS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Protokollgrundlagen und Schutzmechanismen	TLS, SSH, IPsec, Zertifikate, Aushandlung	Vermittelt werden Funktionsweise, Einsatzgrenzen und Sicherheitsgewinne gängiger sicherer Netzwerkprotokolle. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

Fehlkonfigurationen und Angriffsflächen	Unsichere Cipher Suites, Altprotokolle, Downgrade, Missbrauch	Behandelt wird, wie Protokollfehler, Kompatibilitätszwänge oder schwache Implementierungen zu realen Risiken werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie Secure Network Protocols an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 57 KERNELEMENTE UND LERNERGEBNISSE SECURE NETWORK PROTOCOLS

Kernelement	Lernergebnisse
Protokollverständnis	Die Teilnehmenden erklären Aufbau und Schutzwirkung sicherer Netzwerkprotokolle und ordnen deren Einsatzkontexte ein. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Sichere Konfiguration	Die Teilnehmenden erkennen typische Protokollschwächen und formulieren Anforderungen für eine sichere Konfiguration. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Secure Network Protocols so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.8 Fundamentals of SIEM Technology

Fundamentals of SIEM Technology vermittelt die Grundprinzipien von Security Information and Event Management. Im Zentrum stehen Datenquellen, Korrelation, Alarmierung, Aufbewahrung und die Rolle von SIEM-Plattformen als Kernkomponente für Lagebild, Detektion und Nachvollziehbarkeit.

Im Vordergrund steht das Verständnis, wie Datenquellen, Normalisierung, Korrelation, Use Cases und Alarmierung zusammenwirken. Damit wird die Grundlage geschaffen, SIEM nicht nur zu bedienen, sondern als operatives Führungs- und Analyseinstrument zielgerichtet einzusetzen.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 58 WISSENSEINHEITEN UND THEMEN FUNDAMENTALS OF SIEM TECHNOLOGY

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
SIEM-Architektur und Datenquellen	Logquellen, Collector, Parser, Normalisierung, Aufbewahrung	Behandelt wird, welche Bausteine ein SIEM ausmachen und wie sicherheitsrelevante Daten in eine auswertbare Form überführt werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Korrelation und Alarmierung	Regeln, Use Cases, Priorisierung, False Positives	Vermittelt wird, wie aus Einzelereignissen verwertbare Sicherheitsmeldungen entstehen und wie deren Qualität verbessert wird. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Use Cases, Korrelation und Eskalation	Analytische Use Cases, Korrelation, Alarmwege, Nachsteuerung	Behandelt wird, wie Fundamentals of SIEM Technology in konkrete Use Cases, priorisierte Erkennungen und saubere Übergaben an Analyse-, Eskalations- und Reaktionsprozesse überführt wird. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 59 KERNELEMENTE UND LERNERGEBNISSE FUNDAMENTALS OF SIEM TECHNOLOGY

Kernelement	Lernergebnisse
Technologiebasis	Die Teilnehmenden erklären Aufbau, Zweck und Grenzen von SIEM-Systemen im militärischen SOC-/NOC-Kontext. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Operativer Nutzen	Die Teilnehmenden leiten sinnvolle Datenquellen und grundlegende Use Cases für Überwachung und Detektion ab. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Fundamentals of SIEM Technology so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.9 Incident Response and Forensic Analysis

Dieses Wissensgebiet verbindet strukturierte Reaktion auf Sicherheitsvorfälle mit den Grundlagen forensischer Analyse. Es stellt sicher, dass Vorfälle nicht nur eingedämmt, sondern auch in Ursache, Ablauf, Beweislage und Wirkung nachvollzogen werden können.



Das Wissensgebiet verbindet strukturierte Reaktionsabläufe mit der Fähigkeit, Befunde beweissicher zu sichern und zeitlich einzuordnen. In militärischen Umgebungen kommt hinzu, dass Gegenmaßnahmen oft mit betrieblichen Abhängigkeiten, Führungsfreigaben und Eskalationswegen abgestimmt werden müssen.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 60 WISSENSEINHEITEN UND THEMEN INCIDENT RESPONSE AND FORENSIC ANALYSIS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Incident-Response-Prozess	Erkennung, Klassifikation, Eindämmung, Wiederherstellung	Behandelt werden standardisierte Abläufe, Rollen und Entscheidungslogiken für die koordinierte Reaktion auf Sicherheitsvorfälle. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Forensische Grundprinzipien	Spurensicherung, Beweissicherung, Timeline, Analyse	Vermittelt werden Methoden, um artefaktbasiert zu arbeiten, Ergebnisse nachvollziehbar zu dokumentieren und Folgemaßnahmen zu unterstützen. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Operative Integration im Lagebetrieb	Priorisierung, Lagebezug, Berichtswesen, Schnittstellen	Vermittelt wird, wie Ergebnisse aus Incident Response and Forensic Analysis in den laufenden Lage- und Schichtbetrieb integriert und für Führungs- und Entscheidungsprozesse nutzbar gemacht werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 61 KERNELEMENTE UND LERNERGEBNISSE INCIDENT RESPONSE AND FORENSIC ANALYSIS

Kernelement	Lernergebnisse
Koordinierte Reaktion	Die Teilnehmenden wenden Incident-Response-Schritte strukturiert an und stimmen technische wie organisatorische Maßnahmen aufeinander ab. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Nachvollziehbare Analyse	Die Teilnehmenden sichern und analysieren relevante Artefakte so, dass Ursache und Verlauf eines Vorfalls belastbar

	rekonstruiert werden können. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Incident Response and Forensic Analysis so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.10 Tool Assistance

Tool Assistance behandelt den zielgerichteten Einsatz unterstützender Werkzeuge in Analyse, Überwachung und Reaktion. Dazu zählen Automatisierung, Orchestrierung, Unterstützung durch Analysehilfen und die kritische Bewertung, wann Werkzeugunterstützung Sicherheit erhöht und wann sie Fehlsteuerungen begünstigt.

Werkzeuge werden nicht isoliert betrachtet, sondern als Unterstützung für Analysequalität, Geschwindigkeit und Nachvollziehbarkeit. Die Ausbildung legt deshalb Wert darauf, die Grenzen, Voraussetzungen und Fehlermöglichkeiten automatisierter Hilfsmittel transparent zu machen.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 62 WISSENSEINHEITEN UND THEMEN TOOL ASSISTANCE

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Werkzeuggestützte Arbeitsabläufe	Automatisierung, Orchestrierung, Hilfsskripte, Playbooks	Vermittelt wird, wie Tools Prozesse beschleunigen, Standardisierung unterstützen und menschliche Kapazitäten entlasten können. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Grenzen und Qualitätssicherung	Verifikation, Fehlalarme, Transparenz, Kontrollpunkte	Behandelt wird, wie Ergebnisse verifiziert, Fehlsteuerungen vermieden und der Mensch als verantwortliche Entscheidungsinstanz eingebunden bleibt. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Operative Einbettung	Anwendungsfälle, Schnittstellen, Eskalation, Nachweise	Behandelt wird, wie Tool Assistance im militärischen SOC-/NOC-Betrieb praktisch angewendet, mit benachbarten Prozessen verzahnt und nachvollziehbar dokumentiert wird. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb,

		Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 63 KERNELEMENTE UND LERNERGEBNISSE TOOL ASSISTANCE

Kernelement	Lernergebnisse
Sinnvoller Werkzeugeinsatz	Die Teilnehmenden wählen Hilfswerkzeuge passend zu Lage, Reifegrad und Risiko aus und bewerten ihren Mehrwert realistisch. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Verantwortete Automatisierung	Die Teilnehmenden kombinieren Automatisierung mit Kontrollmechanismen, sodass Nachvollziehbarkeit und Eingriffsmöglichkeiten erhalten bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Tool Assistance so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.11 Security Architecture Vulnerabilities

Security Architecture Vulnerabilities fokussiert strukturelle Schwächen von System- und Netzwerkarchitekturen. Im Zentrum stehen Fehlannahmen, unsichere Vertrauensbeziehungen, unzureichende Segmentierung und Designentscheidungen, die Angreifern Bewegung, Eskalation oder Persistenz erleichtern.

Architekturbedingte Schwächen entstehen häufig an Übergängen, Vertrauensannahmen und historisch gewachsenen Kopplungen. Das Wissensgebiet hilft, solche strukturellen Risiken zu erkennen und gegen kurzfristige Einzelmaßnahmen abzuwägen.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 64 WISSENSEINHEITEN UND THEMEN SECURITY ARCHITECTURE VULNERABILITIES

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Architekturbedingte Schwachstellen	Vertrauenszonen, Segmentierung, Single Points of Failure, Exposure	Behandelt werden typische Architekturfehler und ihre Auswirkungen auf Angriffspfad, Erkennbarkeit und Betriebsstabilität. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

Architekturbezogene Abhilfen	Defense in Depth, Zonenmodelle, Redundanz, Härtung	Vermittelt werden Gestaltungsprinzipien, mit denen strukturelle Risiken frühzeitig reduziert und Angriffswege erschwert werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie Security Architecture Vulnerabilities an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 65 KERNELEMENTE UND LERNERGEBNISSE SECURITY ARCHITECTURE VULNERABILITIES

Kernelement	Lernergebnisse
Architekturanalyse	Die Teilnehmenden identifizieren architekturbedingte Schwächen und ordnen deren Einfluss auf Risiko und Betrieb ein. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Sichere Gestaltung	Die Teilnehmenden formulieren Verbesserungen für Segmentierung, Vertrauensbeziehungen und Widerstandsfähigkeit von Architekturen. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Security Architecture Vulnerabilities so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.12 Log Data Analysis Techniques

Log Data Analysis Techniques behandelt Methoden, mit denen Ereignis- und Protokolldaten effizient gefiltert, korreliert, verdichtet und interpretiert werden. Das Wissensgebiet bildet eine Kernfähigkeit für Detektion, Forensik, Betriebstransparenz und die Rekonstruktion von Vorfallverläufen.

Im Zentrum stehen Verfahren, mit denen aus großen Mengen heterogener Protokolldaten belastbare analytische Aussagen gewonnen werden. Das umfasst technische Korrelation ebenso wie Hypothesenbildung, Priorisierung und die nachvollziehbare Dokumentation von Befunden.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und

Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 66 WISSENSEINHEITEN UND THEMEN LOG DATA ANALYSIS TECHNIQUES

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Aufbereitung und Korrelation	Parsing, Normalisierung, Zeitbezug, Kontextanreicherung	Vermittelt wird, wie heterogene Logs in eine gemeinsame analytische Sicht überführt und aussagekräftig verknüpft werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Mustererkennung und Hypothesenprüfung	Baselines, Abweichungen, Suchstrategien, Triagierung	Behandelt wird, wie aus Logdaten belastbare Hypothesen zu Ursache, Relevanz und Umfang sicherheitsrelevanter Ereignisse abgeleitet werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Use Cases, Korrelation und Eskalation	Analytische Use Cases, Korrelation, Alarmwege, Nachsteuerung	Behandelt wird, wie Log Data Analysis Techniques in konkrete Use Cases, priorisierte Erkennungen und saubere Übergaben an Analyse-, Eskalations- und Reaktionsprozesse überführt wird. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 67 KERNELEMENTE UND LERNERGEBNISSE LOG DATA ANALYSIS TECHNIQUES

Kernelement	Lernergebnisse
Analytische Methodik	Die Teilnehmenden wenden geeignete Techniken an, um Logdaten strukturiert zu durchsuchen, zu korrelieren und zu interpretieren. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Bewertbare Befunde	Die Teilnehmenden gewinnen aus Logdaten belastbare Befunde und grenzen Fehlalarme, Störungen und echte Sicherheitsereignisse voneinander ab. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Log Data Analysis Techniques so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.13 Data Collection and Processing

Dieses Wissensgebiet behandelt die systematische Erhebung, Bereinigung, Strukturierung und Verarbeitung sicherheitsrelevanter Daten aus unterschiedlichen Quellen. Es schafft die Voraussetzung dafür, dass Analyse und Lagebild auf konsistenten, belastbaren und zweckmäßigen Datengrundlagen beruhen.

Die Qualität der Datengrundlage entscheidet wesentlich darüber, ob Monitoring, Lagebild und Analyse überhaupt tragfähig sind. Deshalb werden Erhebung, Selektion, Normalisierung und Kontextanreicherung als eigenständige Sicherheitsaufgabe verstanden.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 68 WISSENS-EINHEITEN UND THEMEN DATA COLLECTION AND PROCESSING

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Datenerhebung und Qualität	Quellen, Formate, Vollständigkeit, Konsistenz, Herkunft	Behandelt wird, welche Daten benötigt werden, wie sie erhoben werden und wie ihre Qualität und Verlässlichkeit beurteilt werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Verarbeitung und Anreicherung	Filterung, Transformation, Aggregation, Kontext, Speicherung	Vermittelt wird, wie Rohdaten in nutzbare Datensätze überführt werden, die analytische und operative Fragestellungen unterstützen. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Use Cases, Korrelation und Eskalation	Analytische Use Cases, Korrelation, Alarmwege, Nachsteuerung	Behandelt wird, wie Data Collection and Processing in konkrete Use Cases, priorisierte Erkennungen und saubere Übergaben an Analyse-, Eskalations- und Reaktionsprozesse überführt wird. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 69 KERNELEMENTE UND LERNERGEBNISSE DATA COLLECTION AND PROCESSING

Kernelement	Lernergebnisse
Belastbare Datengrundlage	Die Teilnehmenden stellen sicher, dass für Analyse und Monitoring vollständige, relevante und nachvollziehbare Daten bereitstehen. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

Zweckgerichtete Verarbeitung	Die Teilnehmenden strukturieren und verarbeiten Daten so, dass daraus operative Erkenntnisse effizient gewonnen werden können. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Data Collection and Processing so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.14 Data Visualization and Communication

Data Visualization and Communication fokussiert die Aufbereitung komplexer technischer Informationen für unterschiedliche Zielgruppen. Im Mittelpunkt stehen Visualisierung, Verdichtung, narrative Struktur und die Fähigkeit, aus Daten handlungsrelevante Botschaften für Schichtbetrieb, Führung und Stäbe abzuleiten.

Sicherheitsarbeit endet nicht mit der Analyse; Erkenntnisse müssen für Schichtbetrieb, Führung und Schnittstellenpartner verständlich und handlungsrelevant aufbereitet werden. Gute Visualisierung reduziert Komplexität, ohne kritische Unsicherheiten oder Annahmen zu verdecken.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 70 WISSENSEINHEITEN UND THEMEN DATA VISUALIZATION AND COMMUNICATION

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Visualisierung und Verdichtung	Dashboards, Diagramme, Lagebilder, Trends, Prioritäten	Behandelt wird, wie technische Daten so visualisiert werden, dass Lage, Risiken und Handlungsbedarf schnell erfassbar werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Adressatengerechte Kommunikation	Kurzberichte, Lagevorträge, Unsicherheiten, Empfehlungen	Vermittelt wird, wie Analyseergebnisse für unterschiedliche Ebenen verständlich formuliert und mit klaren Aussagen verbunden werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Use Cases, Korrelation und Eskalation	Analytische Use Cases, Korrelation, Alarmwege, Nachsteuerung	Behandelt wird, wie Data Visualization and Communication in konkrete Use Cases, priorisierte Erkennungen und saubere Übergaben an Analyse-, Eskalations- und Reaktionsprozesse überführt wird. Besonderes Gewicht

		liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 71 KERNELEMENTE UND LERNERGEBNISSE DATA VISUALIZATION AND COMMUNICATION

Kernelement	Lernergebnisse
Darstellungsfähigkeit	Die Teilnehmenden wählen Visualisierungsformen, die technische Komplexität reduzieren, ohne relevante Informationen zu verlieren. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Kommunikationswirksamkeit	Die Teilnehmenden bereiten Erkenntnisse für Schichtbetrieb und Führung so auf, dass daraus belastbare Entscheidungen unterstützt werden. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Data Visualization and Communication so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.15 *Event Monitoring and Threat Detection*

Event Monitoring and Threat Detection verbindet kontinuierliche Überwachung mit der Erkennung sicherheitsrelevanter Muster in Echt- oder Nahechtzeit. Das Wissensgebiet schafft die operative Basis dafür, Vorfälle frühzeitig zu entdecken, zu priorisieren und in einen strukturierten Reaktionsprozess zu überführen.

Im Fokus steht der Übergang von roher Telemetrie zu belastbaren Erkennungen und priorisierten Reaktionen. Dafür müssen Signale, Korrelationen, Schwellenwerte und Verhaltensmuster in den konkreten Betriebs- und Missionskontext eingeordnet werden.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 72 WISSENSEINHEITEN UND THEMEN EVENT MONITORING AND THREAT DETECTION

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Kontinuierliches Monitoring	Sensorik, Telemetrie, Alarme, Schwellenwerte, Betriebsbilder	Behandelt wird der Aufbau einer Überwachungssicht, die sowohl Sicherheitsereignisse als auch betriebliche Anomalien sichtbar macht. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

Threat Detection	Use Cases, Signaturen, Verhalten, Korrelation, Priorisierung	Vermittelt werden Verfahren zur Erkennung bekannter und unbekannter Angriffe sowie zur Bewertung ihrer operativen Relevanz. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Use Cases, Korrelation und Eskalation	Analytische Use Cases, Korrelation, Alarmwege, Nachsteuerung	Behandelt wird, wie Event Monitoring and Threat Detection in konkrete Use Cases, priorisierte Erkennungen und saubere Übergaben an Analyse-, Eskalations- und Reaktionsprozesse überführt wird. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 73 KERNELEMENTE UND LERNERGEBNISSE EVENT MONITORING AND THREAT DETECTION

Kernelement	Lernergebnisse
Früherkennung	Die Teilnehmenden definieren Überwachungs- und Detektionsmechanismen, die sicherheitsrelevante Ereignisse zeitnah sichtbar machen. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Priorisierte Weiterverarbeitung	Die Teilnehmenden unterscheiden zwischen kritischen Vorfällen, technischen Störungen und wenig relevanten Meldungen und leiten passende Reaktionen ein. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Event Monitoring and Threat Detection so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.3.16 Cryptography

Cryptography vermittelt die Grundlagen und den operativen Einsatz kryptographischer Verfahren zum Schutz von Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit. Im militärischen Kontext ist dabei neben der Theorie insbesondere der sichere und zweckmäßige Einsatz in realen Infrastrukturen entscheidend.

Kryptographische Mechanismen werden dabei als grundlegende Enabler für Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit behandelt. Ebenso wichtig ist das Verständnis, dass Fehlkonfiguration, schlechtes Schlüsselmanagement oder falsche Einsatzannahmen die Schutzwirkung erheblich mindern können.

Für die gemeinsame operationelle Ausbildung von SOC und NOC ist entscheidend, dass das Wissensgebiet in Überwachung, Schichtbetrieb, Eskalation und Zusammenarbeit mit

benachbarten Stellen anschlussfähig bleibt. Vermittelt werden daher nicht nur Begriffe und Verfahren, sondern auch deren Nutzen für Lagebild, Priorisierung, Nachweisführung und belastbare Entscheidungen im laufenden Betrieb.

TABELLE 74 WISSENSEINHEITEN UND THEMEN CRYPTOGRAPHY

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Kryptographische Grundmechanismen	Symmetrisch, asymmetrisch, Hashing, Signaturen, Schlüsselaustausch	Vermittelt wird, welche Grundbausteine kryptographischer Schutzmechanismen existieren und welche Schutzziele sie jeweils unterstützen. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Betriebliche Anwendung	Key Management, Zertifikate, Protokolle, Fehlanwendung	Behandelt wird, wie kryptographische Verfahren sicher eingesetzt, verwaltet und gegen typische Implementierungs- oder Nutzungsfehler abgesichert werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.
Schutzmaßnahmen über den Lebenszyklus	Vorsorge, Härtung, Wiederherstellung, Integritätssicherung	Behandelt wird, wie Maßnahmen aus Cryptography entlang des gesamten Lebenszyklus von Daten, Prozessen oder Diensten geplant, umgesetzt und regelmäßig überprüft werden. Besonderes Gewicht liegt auf der Übertragbarkeit in Schichtbetrieb, Monitoring, Eskalation und nachvollziehbare Dokumentation.

TABELLE 75 KERNELEMENTE UND LERNERGEBNISSE CRYPTOGRAPHY

Kernelement	Lernergebnisse
Funktionales Verständnis	Die Teilnehmenden erklären Wirkprinzip und Grenzen kryptographischer Verfahren und ordnen sie passenden Schutzanforderungen zu. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Sicherer Einsatz	Die Teilnehmenden berücksichtigen Schlüsselmanagement, Protokollkontext und Implementierungsrisiken bei der praktischen Nutzung von Kryptographie. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.
Anwendung im Schicht- und Betriebsprozess	Die Teilnehmenden setzen Cryptography so ein, dass Beobachtungen, Bewertungen und Maßnahmen für Überwachung, Eskalation und Nachweisführung im laufenden SOC-/NOC-Betrieb anschlussfähig bleiben. Sie berücksichtigen dabei Betriebsabhängigkeiten, Eskalationswege und den Bedarf an nachvollziehbarer Dokumentation.

5.7.4 SOC-spezifische Knowledge Areas

Die SOC-spezifischen Wissensgebiete stärken insbesondere jene Fähigkeiten, die für Lageaufklärung, detektionsorientierte Analyse, narrative Aufbereitung und die Einordnung von Cyber-Ereignissen in militärische Wirkzusammenhänge erforderlich sind.

TABELLE 76 SOC-SPEZIFISCHE KNOWLEDGE AREAS

Knowledge Area	Typische Verortung im SOC-Pfad
Threat Intelligence	Qualification Level III Intermediate
Anomaly Identification	Qualification Level III Intermediate
Conflict and Cyberspace	Qualification Level II Fundamentals
Information Warfare	Qualification Level IV Expert
Situational Picture (Battlefield Scenarios)	Qualification Level IV Expert
Log Analysis	Qualification Level IV Expert
Forensic Investigations	Qualification Level V Expert
Response to Cyber Interventions	Qualification Level V Expert

5.7.4.1 Threat Intelligence

Threat Intelligence behandelt die systematische Gewinnung, Bewertung und Nutzung von Informationen über Bedrohungsakteure, deren Motive, Fähigkeiten und Vorgehensweisen. Für das SOC schafft dieses Wissensgebiet die Grundlage, Angriffe nicht nur technisch, sondern auch im Kontext bekannter TTPs und Kampagnen zu interpretieren.

Im SOC-Kontext dient Threat Intelligence dazu, Beobachtungen mit Akteuren, Kampagnen und Taktiken zu verknüpfen und dadurch Prioritäten zu schärfen. Sie verbindet externe Informationen mit internen Befunden und verbessert so Lagebewertung, Detektion und Vorbereitung von Gegenmaßnahmen.

Im SOC-spezifischen Teil liegt der Fokus darauf, technische Befunde in ein belastbares Lageverständnis zu überführen und für Detektion, Analyse und Reaktion nutzbar zu machen. Die Teilnehmenden sollen dabei lernen, Unsicherheit systematisch zu behandeln, Beobachtungen zu priorisieren und Ergebnisse adressatengerecht an Führung, Partnerstellen und Einsatzverantwortliche zu kommunizieren.

TABELLE 77 WISSENSEINHEITEN UND THEMEN THREAT INTELLIGENCE

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Quellen und Gewinnung	Feeds, Berichte, Malware-Analysen, Open Sources, Sharing	Behandelt wird, welche Quellen für Threat Intelligence geeignet sind und wie ihre Qualität, Aktualität und Relevanz bewertet werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Einordnung und Nutzung	TTPs, Akteursprofile, Priorisierung, Detection Engineering	Vermittelt wird, wie Informationen über Angreifer in Use Cases, Hypothesen, Warnungen und Schutzmaßnahmen überführt werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

Operative Integration im Lagebetrieb	Priorisierung, Lagebezug, Berichtswesen, Schnittstellen	Vermittelt wird, wie Ergebnisse aus Threat Intelligence in den laufenden Lage- und Schichtbetrieb integriert und für Führungs- und Entscheidungsprozesse nutzbar gemacht werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

TABELLE 78 KERNELEMENTE UND LERNERGEBNISSE THREAT INTELLIGENCE

Kernelement	Lernergebnisse
Kontextualisierung von Bedrohungen	Die Teilnehmenden ordnen technische Beobachtungen bekannten Akteuren, Kampagnen oder Vorgehensmustern zu. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Operative Nutzarmachung	Die Teilnehmenden nutzen Threat Intelligence zur Priorisierung, Detektionsverbesserung und Lageeinschätzung im SOC. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lage- und Führungsrelevanz	Die Teilnehmenden ordnen Ergebnisse aus Threat Intelligence in den Lagekontext ein, priorisieren sie nachvollziehbar und bereiten sie für koordinierte Entscheidungen und Reaktionen des SOC auf. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.

5.7.4.2 Anomaly Identification

Anomaly Identification fokussiert das Erkennen von Abweichungen vom erwarteten Verhalten in Daten, Diensten und Abläufen. Es ergänzt signaturbasierte Detektion um verhaltensorientierte Methoden und hilft, neuartige, versteckte oder langsame Angriffe frühzeitig sichtbar zu machen.

Anomalien sind nur dann nutzbar, wenn sie gegen ein verstandenes Normalverhalten, technische Kontexte und operative Prioritäten bewertet werden. Das Wissensgebiet schult daher auch den Umgang mit Unsicherheit, Fehlalarmen und situationsabhängiger Interpretation.

Im SOC-spezifischen Teil liegt der Fokus darauf, technische Befunde in ein belastbares Lageverständnis zu überführen und für Detektion, Analyse und Reaktion nutzbar zu machen. Die Teilnehmenden sollen dabei lernen, Unsicherheit systematisch zu behandeln, Beobachtungen zu priorisieren und Ergebnisse adressatengerecht an Führung, Partnerstellen und Einsatzverantwortliche zu kommunizieren.

TABELLE 79 WISSENSEINHEITEN UND THEMEN ANOMALY IDENTIFICATION

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Anomaliebegriffe und Baselines	Normalverhalten, Schwellenwerte, saisonale Muster, Kontext	Vermittelt wird, wie Normalzustände bestimmt werden und warum ohne Kontext aus Auffälligkeiten noch keine belastbaren Vorfälle werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in

		Analyseschritte und Meldeprozesse verknüpft.
Methoden der Anomalieerkennung	Statistik, Heuristiken, Verhalten, Streaming, Triage	Behandelt werden Verfahren, mit denen Abweichungen in großen Datenmengen erkannt und in operative Hypothesen überführt werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Operative Integration im Lagebetrieb	Priorisierung, Lagebezug, Berichtswesen, Schnittstellen	Vermittelt wird, wie Ergebnisse aus Anomaly Identification in den laufenden Lage- und Schichtbetrieb integriert und für Führungs- und Entscheidungsprozesse nutzbar gemacht werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

TABELLE 80 KERNELEMENTE UND LERNERGEBNISSE ANOMALY IDENTIFICATION

Kernelement	Lernergebnisse
Abweichungserkennung	Die Teilnehmenden identifizieren auffällige Muster und grenzen betriebliche Besonderheiten von sicherheitsrelevanten Anomalien ab. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Bewertung unter Unsicherheit	Die Teilnehmenden priorisieren Anomalien anhand Kontext, Kritikalität und Plausibilität und leiten weitere Analyseschritte ab. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lage- und Führungsrelevanz	Die Teilnehmenden ordnen Ergebnisse aus Anomaly Identification in den Lagekontext ein, priorisieren sie nachvollziehbar und bereiten sie für koordinierte Entscheidungen und Reaktionen des SOC auf. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.

5.7.4.3 Conflict and Cyberspace

Conflict and Cyberspace ordnet Cyber-Ereignisse in den größeren Kontext von Konflikt, Wettbewerb, Abschreckung und hybriden Bedrohungen ein. Das Wissensgebiet schafft ein Verständnis dafür, wie technische Vorfälle mit politisch-strategischen Zielen, Einflussnahme und militärischer Operationsführung verknüpft sein können.

Cyberspace wird hier als Teil eines erweiterten Konfliktraums verstanden, in dem technische Ereignisse politische, militärische und informationsbezogene Wirkungen entfalten können. Die Ausbildung unterstützt damit die Fähigkeit, Einzelereignisse nicht nur technisch, sondern lagebezogen zu bewerten.

Im SOC-spezifischen Teil liegt der Fokus darauf, technische Befunde in ein belastbares Lageverständnis zu überführen und für Detektion, Analyse und Reaktion nutzbar zu machen. Die Teilnehmenden sollen dabei lernen, Unsicherheit systematisch zu behandeln, Beobachtungen zu

priorisieren und Ergebnisse adressatengerecht an Führung, Partnerstellen und Einsatzverantwortliche zu kommunizieren.

TABELLE 81 WISSENSEINHEITEN UND THEMEN CONFLICT AND CYBERSPACE

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Cyberspace als Konfliktraum	Akteure, Interessen, Eskalation, Hybridität, Wirkdimensionen	Behandelt wird, wie sich staatliche und nichtstaatliche Akteure im Cyber- und Informationsraum positionieren und welche Zielbilder ihr Handeln prägen. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Operative Relevanz für das SOC	Lageeinordnung, Attribution, Wirkung, Berichtswesen	Vermittelt wird, wie technische Beobachtungen in größere Lagezusammenhänge eingeordnet und für Führungsebenen relevant gemacht werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Operative Integration im Lagebetrieb	Priorisierung, Lagebezug, Berichtswesen, Schnittstellen	Vermittelt wird, wie Ergebnisse aus Conflict and Cyberspace in den laufenden Lage- und Schichtbetrieb integriert und für Führungs- und Entscheidungsprozesse nutzbar gemacht werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

TABELLE 82 KERNELEMENTE UND LERNERGEBNISSE CONFLICT AND CYBERSPACE

Kernelement	Lernergebnisse
Strategische Einordnung	Die Teilnehmenden erklären, wie Cyber-Ereignisse Teil umfassender Konfliktdynamiken und hybrider Operationsformen sein können. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lagebezogene Bewertung	Die Teilnehmenden berücksichtigen strategische und politische Dimensionen bei der Analyse und Berichterstattung sicherheitsrelevanter Ereignisse. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lage- und Führungsrelevanz	Die Teilnehmenden ordnen Ergebnisse aus Conflict and Cyberspace in den Lagekontext ein, priorisieren sie nachvollziehbar und bereiten sie für koordinierte Entscheidungen und Reaktionen des SOC auf. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.

5.7.4.4 Information Warfare

Information Warfare beleuchtet den Einsatz von Information, Desinformation und kognitiver Beeinflussung als Teil moderner Konfliktführung. Für das SOC ist dieses Wissensgebiet wichtig, um technische Hinweise, Informationsoperationen und narrative Effekte nicht getrennt, sondern als zusammenhängendes Lagebild zu verstehen.

Behandelt werden Formen gezielter Einflussnahme, Desinformation und narrativer Operationsführung sowie ihre Verbindung zu technischen Operationen. Für das SOC ist diese Perspektive wichtig, weil Informationsoperationen häufig parallel zu Cybervorfällen verlaufen und deren Wirkung verstärken können.

Im SOC-spezifischen Teil liegt der Fokus darauf, technische Befunde in ein belastbares Lageverständnis zu überführen und für Detektion, Analyse und Reaktion nutzbar zu machen. Die Teilnehmenden sollen dabei lernen, Unsicherheit systematisch zu behandeln, Beobachtungen zu priorisieren und Ergebnisse adressatengerecht an Führung, Partnerstellen und Einsatzverantwortliche zu kommunizieren.

TABELLE 83 WISSENSEINHEITEN UND THEMEN INFORMATION WARFARE

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Formen des Informationskriegs	Desinformation, Einflussnahme, Narrative, Täuschung, Koordination	Behandelt werden Mittel und Ziele informationsbezogener Operationen sowie ihre Verbindung zu Cyber-Angriffen und Wahrnehmungsmanagement. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Analyse und Lagebezug	Indikatoren, Quellenkritik, Korrelation, Wirkungseinschätzung	Vermittelt wird, wie Informationen aus technischen und offenen Quellen zusammengeführt werden, um Informationsoperationen einzuordnen. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Verhaltenssteuerung und Kommunikation	SETA, Rollenbilder, Meldewege, Interventionen	Behandelt wird, wie Inhalte aus Information Warfare in sicheres Verhalten, zielgruppengerechte Kommunikation und belastbare Melde- und Unterstützungswege überführt werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

TABELLE 84 KERNELEMENTE UND LERNERGEBNISSE INFORMATION WARFARE

Kernelement	Lernergebnisse
Erweitertes Lageverständnis	Die Teilnehmenden erkennen, wie informationsbezogene Maßnahmen technische Vorfälle begleiten, vorbereiten oder

	verstärken können. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Analytische Einbindung	Die Teilnehmenden integrieren Aspekte von Informationskrieg in Lagebilder, Bewertungen und Entscheidungsvorlagen des SOC. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lage- und Führungsrelevanz	Die Teilnehmenden ordnen Ergebnisse aus Information Warfare in den Lagekontext ein, priorisieren sie nachvollziehbar und bereiten sie für koordinierte Entscheidungen und Reaktionen des SOC auf. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.

5.7.4.5 Situational Picture

Dieses Wissensgebiet behandelt die Verdichtung technischer, organisatorischer und operativer Informationen zu einem belastbaren Lagebild in militärischen Szenarien. Es verbindet Cyber-Ereignisse mit Auftrag, Gelände, Operationsrhythmus und Führungsbedarf und schließt damit die Lücke zwischen Analyse und Entscheidung.

Das Lagebild in Battlefield-Szenarien verlangt die Zusammenführung technischer, operationeller und zeitkritischer Informationen. Ziel ist es, auch unter Unsicherheit ein Bild zu erzeugen, das Auswirkungen, Prioritäten und Handlungsoptionen für Führungsebenen sichtbar macht.

Im SOC-spezifischen Teil liegt der Fokus darauf, technische Befunde in ein belastbares Lageverständnis zu überführen und für Detektion, Analyse und Reaktion nutzbar zu machen. Die Teilnehmenden sollen dabei lernen, Unsicherheit systematisch zu behandeln, Beobachtungen zu priorisieren und Ergebnisse adressatengerecht an Führung, Partnerstellen und Einsatzverantwortliche zu kommunizieren.

TABELLE 85 WISSENSEINHEITEN UND THEMEN SITUATIONAL PICTURE

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Lagebildaufbau	Datenfusion, Zeitbezug, Kritikalität, Handlungsoptionen	Behandelt wird, wie aus verstreuten Informationen eine kohärente und entscheidungsrelevante Gesamtsicht aufgebaut wird. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Battlefield-Kontext	Mission, Wirkung, Verbundsysteme, Prioritäten, Unsicherheiten	Vermittelt wird, wie Cyber-Lagen auf operative Szenarien und deren Risiken bezogen werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Operative Integration im Lagebetrieb	Priorisierung, Lagebezug, Berichtswesen, Schnittstellen	Vermittelt wird, wie Ergebnisse aus Situational Picture (Battlefield Szenarios) in den laufenden Lage- und Schichtbetrieb integriert und für Führungs- und Entscheidungsprozesse nutzbar gemacht werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung

		und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

TABELLE 86 KERNELEMENTE UND LERNERGEBNISSE SITUATIONAL PICTURE

Kernelement	Lernergebnisse
Integrierte Lagewahrnehmung	Die Teilnehmenden erzeugen Lagebilder, die technische Befunde, Missionsbezug und Handlungsoptionen konsistent zusammenführen. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Führungsunterstützung	Die Teilnehmenden kommunizieren Lageinformationen so, dass Kommandeure und Stäbe Entscheidungen unter Unsicherheit fundiert vorbereiten können. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lage- und Führungsrelevanz	Die Teilnehmenden ordnen Ergebnisse aus Situational Picture (Battlefield Scenarios) in den Lagekontext ein, priorisieren sie nachvollziehbar und bereiten sie für koordinierte Entscheidungen und Reaktionen des SOC auf. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.

5.7.4.6 Log Analysis

Log Analysis fokussiert die inhaltliche Auswertung von Protokollen als Kernarbeit des SOC. Das Wissensgebiet verbindet Datenkenntnis mit Hypothesenbildung, Kontextualisierung und der Fähigkeit, Einzelspuren zu Angriffspfaden, Ursachenbildern und priorisierten Handlungsoptionen zu verdichten.

Im Unterschied zur allgemeinen Logdatenanalyse liegt der Schwerpunkt hier auf der tiefenfallbezogenen Untersuchung im Vorfallkontext. Protokolle werden genutzt, um Abläufe zu rekonstruieren, Hypothesen zu prüfen und Eskalationsentscheidungen zu stützen.

Im SOC-spezifischen Teil liegt der Fokus darauf, technische Befunde in ein belastbares Lageverständnis zu überführen und für Detektion, Analyse und Reaktion nutzbar zu machen. Die Teilnehmenden sollen dabei lernen, Unsicherheit systematisch zu behandeln, Beobachtungen zu priorisieren und Ergebnisse adressatengerecht an Führung, Partnerstellen und Einsatzverantwortliche zu kommunizieren.

TABELLE 87 WISSENSEINHEITEN UND THEMEN LOG ANALYSIS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Quellen- und Ereignisverständnis	Systemlogs, Netzlogs, Applikationslogs, Artefakte, Zeitbezug	Behandelt wird, welche Informationen Logs enthalten, wie sie interpretiert werden und welche Grenzen sie besitzen. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Analytische Vertiefung	Pivoting, Timelines, Korrelation, Hypothesenprüfung, Reporting	Vermittelt werden Vorgehensweisen, mit denen aus Protokollspuren verwertbare Erkenntnisse und handlungsrelevante Bewertungen

		entstehen. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Use Cases, Korrelation und Eskalation	Analytische Use Cases, Korrelation, Alarmwege, Nachsteuerung	Behandelt wird, wie Log Analysis in konkrete Use Cases, priorisierte Erkennungen und saubere Übergaben an Analyse-, Eskalations- und Reaktionsprozesse überführt wird. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

TABELLE 88 KERNELEMENTE UND LERNERGEBNISSE LOG ANALYSIS

Kernelement	Lernergebnisse
Tiefgehende Analysefähigkeit	Die Teilnehmenden lesen und interpretieren Protokolle auch in komplexen, mehrstufigen Vorfalllagen sicher und strukturiert. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Ableitbare Maßnahmen	Die Teilnehmenden leiten aus Logbefunden Prioritäten, Eskalationen und konkrete Reaktionsmaßnahmen ab. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lage- und Führungsrelevanz	Die Teilnehmenden ordnen Ergebnisse aus Log Analysis in den Lagekontext ein, priorisieren sie nachvollziehbar und bereiten sie für koordinierte Entscheidungen und Reaktionen des SOC auf. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.

5.7.4.7 Forensic Investigations

Forensic Investigations vertieft die methodische Untersuchung sicherheitsrelevanter Vorfälle mit dem Ziel, Ursache, Verlauf, Umfang und gegebenenfalls Beweislage belastbar zu rekonstruieren. Das Wissensgebiet ist besonders dort relevant, wo aus einem Vorfall strategische, disziplinäre oder rechtliche Folgerungen gezogen werden müssen.

Forensische Untersuchungen dienen nicht nur der Ursachenklärung, sondern auch der belastbaren Rekonstruktion von Angriffspfaden, Wirkungen und Verantwortlichkeiten. Damit sind sie eine Brücke zwischen technischer Analyse, Lessons Learned und ggf. rechtlicher Verwertbarkeit.

Im SOC-spezifischen Teil liegt der Fokus darauf, technische Befunde in ein belastbares Lageverständnis zu überführen und für Detektion, Analyse und Reaktion nutzbar zu machen. Die Teilnehmenden sollen dabei lernen, Unsicherheit systematisch zu behandeln, Beobachtungen zu priorisieren und Ergebnisse adressatengerecht an Führung, Partnerstellen und Einsatzverantwortliche zu kommunizieren.

TABELLE 89 WISSENSEINHEITEN UND THEMEN FORENSIC INVESTIGATIONS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance

Forensischer Untersuchungsprozess	Planung, Sicherung, Kette des Nachweises, Dokumentation	Behandelt wird, wie Untersuchungen vorbereitet, Spuren sauber gesichert und Ergebnisse nachvollziehbar dokumentiert werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Artefakt- und Verlaufsauswertung	Dateien, Speicher, Netzwerkspuren, Malware, Timelines	Vermittelt werden Techniken, um aus Artefakten den Ablauf eines Vorfalls und dessen Wirkung auf Systeme und Daten zu rekonstruieren. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Operative Integration im Lagebetrieb	Priorisierung, Lagebezug, Berichtswesen, Schnittstellen	Vermittelt wird, wie Ergebnisse aus Forensic Investigations in den laufenden Lage- und Schichtbetrieb integriert und für Führungs- und Entscheidungsprozesse nutzbar gemacht werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

TABELLE 90 KERNELEMENTE UND LERNERGEBNISSE FORENSIC INVESTIGATIONS

Kernelement	Lernergebnisse
Methodische Untersuchung	Die Teilnehmenden führen forensische Untersuchungen so durch, dass Ergebnisse reproduzierbar, nachvollziehbar und verwendbar bleiben. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Rekonstruktion und Schlussfolgerung	Die Teilnehmenden rekonstruieren Vorfallverläufe und leiten daraus technische, organisatorische und gegebenenfalls rechtlich relevante Konsequenzen ab. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lage- und Führungsrelevanz	Die Teilnehmenden ordnen Ergebnisse aus Forensic Investigations in den Lagekontext ein, priorisieren sie nachvollziehbar und bereiten sie für koordinierte Entscheidungen und Reaktionen des SOC auf. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.

5.7.4.8 Response to Cyber Interventions

Response to Cyber Interventions behandelt die Planung, Abstimmung und Bewertung von Maßnahmen als Reaktion auf erkannte Cyber-Aktivitäten. Das Wissensgebiet betont die Verbindung zwischen technischer Reaktion, Führungsabsicht, Verhältnismäßigkeit und den möglichen Nebenwirkungen von Eingriffen.

Dieses Wissensgebiet behandelt die Planung, Abstimmung und Bewertung aktiver Reaktionsmaßnahmen. Im Vordergrund steht die Frage, welche technische oder organisatorische Intervention unter gegebenen Risiken, Freigaben und erwarteten Nebenwirkungen vertretbar ist.

Im SOC-spezifischen Teil liegt der Fokus darauf, technische Befunde in ein belastbares Lageverständnis zu überführen und für Detektion, Analyse und Reaktion nutzbar zu machen. Die Teilnehmenden sollen dabei lernen, Unsicherheit systematisch zu behandeln, Beobachtungen zu priorisieren und Ergebnisse adressatengerecht an Führung, Partnerstellen und Einsatzverantwortliche zu kommunizieren.

TABELLE 91 WISSENSEINHEITEN UND THEMEN RESPONSE TO CYBER INTERVENTIONS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Interventionsoptionen	Containment, Isolierung, Täuschung, Umkonfiguration, Eskalation	Behandelt wird, welche Eingriffsmöglichkeiten bestehen und unter welchen Bedingungen sie technisch und operativ sinnvoll sind. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Abstimmung und Wirkung	Freigaben, Nebenwirkungen, Kommunikation, Nachsteuerung	Vermittelt wird, wie Interventionen mit anderen Stellen abgestimmt und hinsichtlich ihrer Folgen kontinuierlich bewertet werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.
Operative Integration im Lagebetrieb	Priorisierung, Lagebezug, Berichtswesen, Schnittstellen	Vermittelt wird, wie Ergebnisse aus Response to Cyber Interventions in den laufenden Lage- und Schichtbetrieb integriert und für Führungs- und Entscheidungsprozesse nutzbar gemacht werden. Im SOC-Kontext wird dies mit Lagebezug, Priorisierung und der Einbindung in Analyseschritte und Meldeprozesse verknüpft.

TABELLE 92 KERNELEMENTE UND LERNERGEBNISSE RESPONSE TO CYBER INTERVENTIONS

Kernelement	Lernergebnisse
Interventionsplanung	Die Teilnehmenden vergleichen Reaktionsoptionen hinsichtlich Wirksamkeit, Risiko, Nebenwirkung und Führungsabsicht. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Verantwortete Umsetzung	Die Teilnehmenden stimmen Cyber-Interventionen mit zuständigen Stellen ab und überwachen ihre Wirkung systematisch. Sie binden ihre Bewertung in Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.
Lage- und Führungsrelevanz	Die Teilnehmenden ordnen Ergebnisse aus Response to Cyber Interventions in den Lagekontext ein, priorisieren sie nachvollziehbar und bereiten sie für koordinierte Entscheidungen und Reaktionen des SOC auf. Sie binden ihre Bewertung in

	Lagearbeit, Priorisierung und koordinierte Reaktionsschritte des SOC ein.

5.7.5 NOC-spezifische Knowledge Areas

Die NOC-spezifischen Wissensgebiete vertiefen insbesondere netzwerkbezogene, betriebsnahe und OT-orientierte Fähigkeiten. Sie unterstützen den sicheren und resilienten Betrieb komplexer Kommunikations- und Infrastruktursysteme unter Normal- und Störungsbedingungen.

TABELLE 93 NOC-SPEZIFISCHE KNOWLEDGE AREAS

Knowledge Area	Typische Verortung im NOC-Pfad
Network Traffic Analysis	Qualification Level III Intermediate
Security Architecture for OT	Qualification Level IV Expert
Security Guidelines and Standards	Qualification Level IV Expert
Network Traffic Activity Detection and Tracking	Qualification Level IV Expert
Detecting CS Attacks	Qualification Level V Expert

5.7.5.1 Network Traffic Analysis

Network Traffic Analysis behandelt die strukturierte Untersuchung von Kommunikationsmustern, Protokollflüssen und Verkehrscharakteristika in Netzen. Für das NOC ist dieses Wissensgebiet zentral, um Betriebszustände zu bewerten, Fehlfunktionen zu diagnostizieren und sicherheitsrelevante Auffälligkeiten mit dem Netzverhalten in Beziehung zu setzen.

Netzverkehr liefert im NOC eine zentrale Beobachtungsgrundlage für Leistung, Stabilität und Sicherheit. Die Analyse verbindet Protokollwissen mit der Fähigkeit, Verkehrsprofile, Engpässe und verdächtige Muster in ihrem operativen Kontext zu interpretieren.

Im NOC-spezifischen Teil werden die Inhalte mit besonderem Blick auf Verfügbarkeit, Stabilität, OT-Nähe und betriebliche Abhängigkeiten vermittelt. Die Teilnehmenden sollen technische Auffälligkeiten nicht nur erkennen, sondern deren Auswirkungen auf Dienste, Verbundsysteme und Wiederherstellungsfähigkeit realistisch bewerten können.

TABELLE 94 WISSENSEINHEITEN UND THEMEN NETWORK TRAFFIC ANALYSIS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Verkehrsbilder und Protokollmuster	Flows, Sessions, Protokollverhalten, Lastprofile, Baselines	Behandelt wird, wie typisches Netzwerkverhalten beschrieben und für Analyse und Überwachung nutzbar gemacht wird. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.
Analyse betrieblicher und sicherheitsrelevanter Auffälligkeiten	Engpässe, Latenz, Scans, C2-Muster, Seitwärtsbewegung	Vermittelt wird, wie Verkehrsbeobachtungen in Hinweise auf Störungen, Fehlkonfigurationen oder Angriffe übersetzt werden. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.

Betriebsnahe Überwachung und Eskalation	Baselines, Auswirkungen, Abstimmung, Wiederanlauf	Behandelt wird, wie Network Traffic Analysis in überwachte Betriebsprozesse eingebettet wird und wie bei Auffälligkeiten abgestimmt, priorisiert und mit Blick auf Verfügbarkeit reagiert wird. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.

TABELLE 95 KERNELEMENTE UND LERNERGEBNISSE NETWORK TRAFFIC ANALYSIS

Kernelement	Lernergebnisse
Verkehrsverständnis	Die Teilnehmenden analysieren Netzwerkverkehr hinsichtlich Normalverhalten, Leistungsmerkmalen und Abweichungen. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Diagnosefähigkeit	Die Teilnehmenden ordnen Verkehrsauffälligkeiten betrieblichen oder sicherheitsrelevanten Ursachen zu und leiten passende Maßnahmen ab. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Betriebs- und Verfügbarkeitsbezug	Die Teilnehmenden bewerten Maßnahmen aus Network Traffic Analysis unter Berücksichtigung von Verfügbarkeit, Betriebsstabilität und Abhängigkeiten zu angrenzenden Diensten oder OT-Komponenten. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.

5.7.5.2 Security Architecture for OT

Security Architecture for OT fokussiert den sicheren architektonischen Aufbau industrieller Steuerungs- und Prozessumgebungen. Das Wissensgebiet verbindet Segmentierung, Fernwartung, Protokollsicherheit und betriebstechnische Randbedingungen zu einem Schutzkonzept, das Sicherheit und Verfügbarkeit gleichermaßen berücksichtigt.

IOT-Architekturen stellen besondere Anforderungen, weil Sicherheitsmaßnahmen mit Safety, Verfügbarkeit, Legacy-Abhängigkeiten und Wartungsrealitäten in Einklang gebracht werden müssen. Architekturentscheidungen wirken sich hier unmittelbar auf Störungsrisiken und Wiederherstellbarkeit aus.

Im NOC-spezifischen Teil werden die Inhalte mit besonderem Blick auf Verfügbarkeit, Stabilität, OT-Nähe und betriebliche Abhängigkeiten vermittelt. Die Teilnehmenden sollen technische Auffälligkeiten nicht nur erkennen, sondern deren Auswirkungen auf Dienste, Verbundsysteme und Wiederherstellungsfähigkeit realistisch bewerten können.

TABELLE 96 WISSENSEINHEITEN UND THEMEN SECURITY ARCHITECTURE FOR OT

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
OT-Architekturprinzipien	Zonen, Conduits, Fernzugriff, Jump Hosts, Trennung	Vermittelt werden Strukturprinzipien, mit denen OT-Umgebungen gegen unbeabsichtigte und gegnerische

		Einwirkungen widerstandsfähiger gemacht werden. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.
Architekturbedingte Betriebsgrenzen	Legacy-Systeme, Echtzeit, Safety, Wartungsfenster, Kompensation	Behandelt wird, wie Sicherheitsmaßnahmen so gewählt werden, dass Betriebs- und Safety-Anforderungen nicht unterlaufen werden. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.
Abhängigkeiten und Schnittstellen	Vertrauensbeziehungen, Übergänge, externe Dienste, Kompensation	Vermittelt wird, wie Security Architecture for OT an Systemgrenzen, Schnittstellen und Abhängigkeiten wirksam wird und welche kompensierenden Maßnahmen an kritischen Übergängen erforderlich sind. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.

TABELLE 97 KERNELEMENTE UND LERNERGEBNISSE SECURITY ARCHITECTURE FOR OT

Kernelement	Lernergebnisse
OT-gerechte Schutzarchitektur	Die Teilnehmenden entwerfen Schutzarchitekturen für OT, die Segmentierung, Zugangskontrolle und Betriebszwänge konsistent verbinden. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Abwägun gsfähigkeit	Die Teilnehmenden bewerten Sicherheitsmaßnahmen für OT unter Berücksichtigung von Verfügbarkeit, Safety und Wartbarkeit. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Betriebs- und Verfügbarkeitsbezug	Die Teilnehmenden bewerten Maßnahmen aus Security Architecture for OT unter Berücksichtigung von Verfügbarkeit, Betriebsstabilität und Abhängigkeiten zu angrenzenden Diensten oder OT-Komponenten. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.

5.7.5.3 Security Guidelines and Standards

Dieses Wissensgebiet behandelt Richtlinien, Standards und Referenzrahmen, die für den sicheren Betrieb von Netzen, Systemen und OT-Umgebungen relevant sind. Es schafft Orientierung für Architekturentscheidungen, Mindestanforderungen, Prüfverfahren und den Nachweis ordnungsgemäßer Umsetzung.

Richtlinien und Standards schaffen einen gemeinsamen Referenzrahmen für Planung, Betrieb, Prüfung und Weiterentwicklung. Die Herausforderung liegt darin, abstrakte Vorgaben in umsetzbare Baselines, Prüfkriterien und betrieblich tragfähige Verfahren zu überführen.

Im NOC-spezifischen Teil werden die Inhalte mit besonderem Blick auf Verfügbarkeit, Stabilität, OT-Nähe und betriebliche Abhängigkeiten vermittelt. Die Teilnehmenden sollen technische Auffälligkeiten nicht nur erkennen, sondern deren Auswirkungen auf Dienste, Verbundsysteme und Wiederherstellungsfähigkeit realistisch bewerten können.

TABELLE 98 WISSENSEINHEITEN UND THEMEN SECURITY GUIDELINES AND STANDARDS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Normen und Referenzrahmen	NIST, ISO, IEC, domänenspezifische Vorgaben, Profile	Behandelt wird, welche Standards in welchen Kontexten Orientierung geben und wie sie in militärische Umgebungen übertragen werden können. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.
Umsetzung in Verfahren und Baselines	Mindeststandards, Checklisten, Prüfungen, Abweichungsmanagement	Vermittelt wird, wie Richtlinien in technische Baselines, Betriebsregeln und nachvollziehbare Nachweisverfahren übersetzt werden. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.
Betriebsnahe Überwachung und Eskalation	Baselines, Auswirkungen, Abstimmung, Wiederanlauf	Behandelt wird, wie Security Guidelines and Standards in überwachte Betriebsprozesse eingebettet wird und wie bei Auffälligkeiten abgestimmt, priorisiert und mit Blick auf Verfügbarkeit reagiert wird. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.

TABELLE 99 KERNELEMENTE UND LERNERGEBNISSE SECURITY GUIDELINES AND STANDARDS

Kernelement	Lernergebnisse
Orientierungswissen	Die Teilnehmenden ordnen relevante Sicherheitsstandards geeigneten Einsatzkontexten zu und erklären deren Nutzen für Betrieb und Prüfung. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Praktische Operationalisierung	Die Teilnehmenden leiten aus Standards konkrete Anforderungen, Baselines und Nachweisverfahren für den NOC-Betrieb ab. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Betriebs- und Verfügbarkeitsbezug	Die Teilnehmenden bewerten Maßnahmen aus Security Guidelines and Standards unter Berücksichtigung von

	Verfügbarkeit, Betriebsstabilität und Abhängigkeiten zu angrenzenden Diensten oder OT-Komponenten. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.

5.7.5.4 Network Traffic Activity Detection and Tracking

Network Traffic Activity Detection and Tracking vertieft die Erkennung und Nachverfolgung konkreter Aktivitäten im Netz. Im Mittelpunkt stehen Verlauf, Ursprung, Richtung, Muster und Persistenz von Kommunikationsbeziehungen sowie deren Nutzung für Lageaufklärung und Reaktionsplanung.

Im Zentrum steht die Fähigkeit, Aktivitäten über Zeit, Systeme und Kommunikationspfade hinweg nachzuverfolgen. Gerade in verteilten Umgebungen ist dieses Tracking entscheidend, um Vorfälle in ihrem Umfang zu erfassen und Folgehandlungen früh zu erkennen.

Im NOC-spezifischen Teil werden die Inhalte mit besonderem Blick auf Verfügbarkeit, Stabilität, OT-Nähe und betriebliche Abhängigkeiten vermittelt. Die Teilnehmenden sollen technische Auffälligkeiten nicht nur erkennen, sondern deren Auswirkungen auf Dienste, Verbundsysteme und Wiederherstellungsfähigkeit realistisch bewerten können.

TABELLE 100 WISSENSEINHEITEN UND THEMEN NETWORK TRAFFIC ACTIVITY DETECTION AND TRACKING

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Erkennung verdächtiger Aktivitäten	Beaconing, Lateral movement, Exfiltration, wiederkehrende Muster	Vermittelt wird, wie charakteristische Aktivitätsmuster im Netzwerk sichtbar gemacht und priorisiert werden. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.
Tracking und Verlaufsketten	Zeitliche Verfolgung, Pivoting, Knotenbeziehungen, Ausbreitung	Behandelt wird, wie Kommunikationspfade und Aktivitätsketten über mehrere Systeme und Zeitpunkte hinweg nachverfolgt werden. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.
Use Cases, Korrelation und Eskalation	Analytische Use Cases, Korrelation, Alarmwege, Nachsteuerung	Behandelt wird, wie Network Traffic Activity Detection and Tracking in konkrete Use Cases, priorisierte Erkennungen und saubere Übergaben an Analyse-, Eskalations- und Reaktionsprozesse überführt wird. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.

TABELLE 101 KERNELEMENTE UND LERNERGEBNISSE NETWORK TRAFFIC ACTIVITY
 DETECTION AND TRACKING

Kernelement	Lernergebnisse
Aktivitätsdetektion	Die Teilnehmenden identifizieren im Verkehrsmuster Hinweise auf laufende oder vorbereitende Angriffsaktivitäten. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Verlaufsrekonstruktion	Die Teilnehmenden verfolgen Kommunikations- und Aktivitätsketten, um Umfang, Richtung und mögliche nächste Schritte eines Angreifers abzuschätzen. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Betriebs- und Verfügbarkeitsbezug	Die Teilnehmenden bewerten Maßnahmen aus Network Traffic Activity Detection and Tracking unter Berücksichtigung von Verfügbarkeit, Betriebsstabilität und Abhängigkeiten zu angrenzenden Diensten oder OT-Komponenten. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.

5.7.5.5 Detecting CS Attacks

Detecting CS Attacks konzentriert sich auf die Erkennung konkreter Cyber-Sicherheitsangriffe im betriebsnahen NOC-Kontext. Es verbindet Sensorik, Verkehrsanalyse, Zustandswissen und Alarmbewertung, um Angriffe gegen Kommunikationsinfrastrukturen und verbundene Dienste frühzeitig sichtbar zu machen.

Die Angriffserkennung im NOC verbindet Musterwissen, Telemetrie und betriebliche Einordnung. Relevante Erkennungen müssen schnell validiert, priorisiert und mit Maßnahmen verbunden werden, ohne dabei Verfügbarkeit und Stabilität aus dem Blick zu verlieren.

Im NOC-spezifischen Teil werden die Inhalte mit besonderem Blick auf Verfügbarkeit, Stabilität, OT-Nähe und betriebliche Abhängigkeiten vermittelt. Die Teilnehmenden sollen technische Auffälligkeiten nicht nur erkennen, sondern deren Auswirkungen auf Dienste, Verbundsysteme und Wiederherstellungsfähigkeit realistisch bewerten können.

TABELLE 102 WISSENSEINHEITEN UND THEMEN DETECTING CS ATTACKS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Angriffsmuster und Indikatoren	DoS, Scans, Manipulation, Missbrauch legitimer Protokolle, OT-Angriffe	Behandelt werden typische Muster, an denen Angriffe auf Netz- und Kommunikationsinfrastrukturen erkannt werden können. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.
Alarmbewertung und Reaktionseinleitung	Validierung, Kontext, Priorisierung, Eskalation, Gegenmaßnahmen	Vermittelt wird, wie aus Erkennungen belastbare Bewertungen entstehen und welche Reaktionsketten daraus folgen. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.

Betriebsnahe Überwachung und Eskalation	Baselines, Auswirkungen, Abstimmung, Wiederanlauf	Behandelt wird, wie Detecting CS Attacks in überwachte Betriebsprozesse eingebettet wird und wie bei Auffälligkeiten abgestimmt, priorisiert und mit Blick auf Verfügbarkeit reagiert wird. Im NOC-Kontext werden zusätzlich Auswirkungen auf Stabilität, Verfügbarkeit und abhängige Systeme berücksichtigt.

TABELLE 103 KERNELEMENTE UND LERNERGEBNISSE DETECTING CS ATTACKS

Kernelement	Lernergebnisse
Angriffserkennung	Die Teilnehmenden erkennen typische technische Muster von Angriffen auf Kommunikations- und Netzwerkinfrastrukturen. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Operatives Handeln	Die Teilnehmenden bewerten Erkennungen im Betriebskontext, priorisieren sie und stoßen angemessene Eskalations- und Reaktionsschritte an. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.
Betriebs- und Verfügbarkeitsbezug	Die Teilnehmenden bewerten Maßnahmen aus Detecting CS Attacks unter Berücksichtigung von Verfügbarkeit, Betriebsstabilität und Abhängigkeiten zu angrenzenden Diensten oder OT-Komponenten. Sie wägen ihre Entscheidungen gegenüber Verfügbarkeit, Safety-nahen Anforderungen und Betriebsfolgen ab.

5.7.6 Optionale Vertiefungen

Die optionalen Vertiefungen erweitern das Curriculum um Fähigkeiten, die je nach Rolle, Vorwissen und Einsatzprofil besonders wertvoll sein können. Sie unterstützen die Professionalisierung in Betrieb, Analyse, Absicherung und prüfender Bewertung technischer Umgebungen.

TABELLE 104 OPTIONALE VERTIEFUNGEN

Knowledge Area	Einordnung
Linux	Optional – SOC
Penetration Testing Fundamentals	Optional – SOC
Penetration Testing Advanced	Optional – SOC
Cryptography	Optional – SOC/NOC

5.7.6.1 Linux

Linux vermittelt die für SOC- und NOC-Personal häufig notwendige Betriebssicherheit im Umgang mit Linux-basierten Systemen. Das Wissensgebiet umfasst Dateisysteme, Prozesse, Dienste, Rechte, Protokollierung und typische Administrations- und Analysewerkzeuge in sicherheitsrelevanten Kontexten.

Linux bildet in vielen Überwachungs-, Analyse- und Serverumgebungen die operative Grundlage. Sichere Bedienung, Diagnosefähigkeit und ein souveräner Umgang mit Shell, Prozessen, Diensten und Logs gehören deshalb zu den praktischen Kernkompetenzen.

In den optionalen Vertiefungen wird das Wissensgebiet in Labor- und Übungsszenarien so ausgebaut, dass aus theoretischem Verständnis belastbare praktische Handlungssicherheit wird. Der Schwerpunkt liegt auf methodischer Sauberkeit, sicherer Durchführung und der Fähigkeit, gewonnene Befunde in konkrete Verbesserungen für Betrieb und Architektur zu übersetzen.

TABELLE 105 WISSENSEINHEITEN UND THEMEN LINUX

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Systemgrundlagen	Dateisystem, Prozesse, Dienste, Nutzer, Rechte	Behandelt werden jene Linux-Konzepte, die für sicheren Betrieb, Fehlersuche und nachvollziehbare Analyse unverzichtbar sind. Die Inhalte werden praxisnah in Labor- und Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.
Sicherheitsrelevante Praxis	Logs, Netzwerkwerkzeuge, Shell, Automatisierung, Hardening	Vermittelt wird, wie Linux-Systeme im Sicherheitsbetrieb beobachtet, abgesichert und analysiert werden können. Die Inhalte werden praxisnah in Labor- und Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.
Praktische Labor- und Übungsumsetzung	Toolchains, Dokumentation, Sicherheit, Auswertung	Vermittelt wird, wie Methoden aus Linux sicher vorbereitet, praktisch durchgeführt und in sauber dokumentierte Ergebnisse mit unmittelbarem Verbesserungswert überführt werden. Die Inhalte werden praxisnah in Labor- und Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.

TABELLE 106 KERNELEMENTE UND LERNERGEBNISSE LINUX

Kernelement	Lernergebnisse
Betriebssicherheit	Die Teilnehmenden arbeiten sicher mit Linux-basierten Systemen und interpretieren grundlegende Betriebs- und Sicherheitsartefakte korrekt. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.
Analytischer Werkzeuggebrauch	Die Teilnehmenden nutzen Linux-typische Werkzeuge für Diagnose, Überwachung und Absicherung zielgerichtet und nachvollziehbar. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.
Methodische Umsetzungskompetenz	Die Teilnehmenden wenden Verfahren aus Linux in praktischen Szenarien sicher an, dokumentieren ihre Schritte nachvollziehbar und leiten aus den Ergebnissen belastbare Verbesserungen ab. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.

5.7.6.2 Penetration Testing Fundamentals

Penetration Testing Fundamentals vermittelt ein grundlegendes Verständnis prüfender Sicherheitsanalysen aus Sicht eines kontrollierten Angriffs. Ziel ist nicht offensive Wirkung, sondern ein besseres Verständnis für Angriffswege, Nachweise, Grenzen und die sichere Einbettung solcher Tests in ein verantwortetes Vorgehen.

Die Grundlagen des Penetration Testings vermitteln einen methodischen Blick auf Angriffsflächen, Schwachstellen und Nachweisführung. Zugleich wird betont, dass prüfende Sicherheitsanalysen klare Regeln, Freigaben und saubere Dokumentation erfordern.

In den optionalen Vertiefungen wird das Wissensgebiet in Labor- und Übungsszenarien so ausgebaut, dass aus theoretischem Verständnis belastbare praktische Handlungssicherheit wird. Der Schwerpunkt liegt auf methodischer Sauberkeit, sicherer Durchführung und der Fähigkeit, gewonnene Befunde in konkrete Verbesserungen für Betrieb und Architektur zu übersetzen.

TABELLE 107 WISSENSEINHEITEN UND THEMEN PENETRATION TESTING FUNDAMENTALS

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Grundlagen und Methodik	Scope, Regeln, Reconnaissance, Nachweisführung, Dokumentation	Behandelt wird, wie Penetration Tests geplant, abgegrenzt und methodisch sauber durchgeführt werden. Die Inhalte werden praxisnah in Labor- und Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.
Basisangriffe und Auswertung	Schwachstellenausnutzung, Fehlkonfigurationen, Priorisierung, Reporting	Vermittelt wird, wie technische Nachweise gewonnen und in umsetzbare Befunde überführt werden. Die Inhalte werden praxisnah in Labor- und Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.
Praktische Labor- und Übungsumsetzung	Toolchains, Dokumentation, Sicherheit, Auswertung	Vermittelt wird, wie Methoden aus Penetration Testing Fundamentals sicher vorbereitet, praktisch durchgeführt und in sauber dokumentierte Ergebnisse mit unmittelbarem Verbesserungswert überführt werden. Die Inhalte werden praxisnah in Labor- und Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.

TABELLE 108 KERNELEMENTE UND LERNERGEBNISSE PENETRATION TESTING FUNDAMENTALS

Kernelement	Lernergebnisse
Verständnis von Angriffspfaden	Die Teilnehmenden erklären typische Schritte eines Penetration Tests und ordnen dessen Nutzen für Sicherheitsverbesserungen ein. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.

Verantwortete Durchführung	Die Teilnehmenden berücksichtigen Scope, Genehmigungen, Risiken und Dokumentation bei grundlegenden prüfenden Sicherheitsanalysen. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.
Methodische Umsetzungskompetenz	Die Teilnehmenden wenden Verfahren aus Penetration Testing Fundamentals in praktischen Szenarien sicher an, dokumentieren ihre Schritte nachvollziehbar und leiten aus den Ergebnissen belastbare Verbesserungen ab. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.

5.7.6.3 Penetration Testing Advanced

Penetration Testing Advanced vertieft komplexere Prüfmethoden, mehrstufige Angriffspfade und die Bewertung architekturbedingter Schwächen. Das Wissensgebiet richtet sich an fortgeschrittene Teilnehmende und unterstützt ein tieferes Verständnis dafür, wie realistische Angreifer Sicherheitsmechanismen umgehen oder kombinieren.

Die fortgeschrittene Vertiefung betrachtet mehrstufige Angriffsketten, Pivoting und das Zusammenspiel mehrerer Schwächen. Ziel ist es, komplexe Prüfergebnisse in robuste Architektur- und Härtingsmaßnahmen zu übersetzen.

In den optionalen Vertiefungen wird das Wissensgebiet in Labor- und Übungsszenarien so ausgebaut, dass aus theoretischem Verständnis belastbare praktische Handlungssicherheit wird. Der Schwerpunkt liegt auf methodischer Sauberkeit, sicherer Durchführung und der Fähigkeit, gewonnene Befunde in konkrete Verbesserungen für Betrieb und Architektur zu übersetzen.

TABELLE 109 WISSENSEINHEITEN UND THEMEN PENETRATION TESTING ADVANCED

Wissenseinheit	Themen	Beschreibung / Curricular Guidance
Komplexe Angriffsketten	Pivoting, Privilege Escalation, laterale Bewegung, Kombinationsangriffe	Behandelt werden fortgeschrittene Vorgehensweisen, mit denen Angreifer mehrere Schwächen verbinden und ihre Position systematisch ausbauen. Die Inhalte werden praxisnah in Labor- und Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.
Architektur- und Wirkungsanalyse	Mehrstufige Szenarien, Sicherheitsgrenzen, Nachweisführung, Maßnahmenableitung	Vermittelt wird, wie fortgeschrittene Prüfergebnisse bewertet und in Architekturverbesserungen und priorisierte Abhilfen übersetzt werden. Die Inhalte werden praxisnah in Labor- und Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.
Praktische Labor- und Übungsumsetzung	Toolchains, Dokumentation, Sicherheit, Auswertung	Vermittelt wird, wie Methoden aus Penetration Testing Advanced sicher vorbereitet, praktisch durchgeführt und in sauber dokumentierte Ergebnisse mit unmittelbarem Verbesserungswert überführt werden. Die Inhalte werden praxisnah in Labor- und

		Übungssettings vertieft, damit ein sicherer Werkzeug- und Methodengebrauch entsteht.

TABELLE 110 KERNELEMENTE UND LERNERGEBNISSE PENETRATION TESTING ADVANCED

Kernelement	Lernergebnisse
Tiefgehendes Angriffsverständnis	Die Teilnehmenden analysieren mehrstufige Angriffsketten und beurteilen deren Relevanz für reale Betriebs- und Einsatzumgebungen. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.
Ableitung von Architekturmaßnahmen	Die Teilnehmenden übersetzen fortgeschrittene Prüfergebnisse in belastbare Härtings-, Segmentierungs- und Überwachungsmaßnahmen. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.
Methodische Umsetzungskompetenz	Die Teilnehmenden wenden Verfahren aus Penetration Testing Advanced in praktischen Szenarien sicher an, dokumentieren ihre Schritte nachvollziehbar und leiten aus den Ergebnissen belastbare Verbesserungen ab. Sie arbeiten methodisch sauber, berücksichtigen Randbedingungen und leiten aus den Ergebnissen konkrete Verbesserungen ab.

Die dargestellten Knowledge Areas bilden zugleich den Referenzrahmen für die Ausgestaltung der Ausbildungsmodule, für Übungs- und Prüfungsformate sowie für die spätere Qualitätssicherung und Fortschreibung des Curriculums.

5.8 Ausbildungsmodule

Die Ausbildungsmodule konkretisieren die im Curriculum definierten Wissensgebiete und überführen diese in eine didaktisch strukturierte sowie organisationspraktisch umsetzbare Lehrgangsarchitektur. Während die Wissensgebiete festlegen, welche fachlichen Domänen und Kompetenzfelder für die Zielrollen relevant sind, bestimmen die Module, in welcher Reihenfolge, mit welchen methodischen Schwerpunkten und in welchen Lernformaten diese Inhalte vermittelt, geübt und überprüft werden. Die modulare Struktur bildet damit die operative Ebene des Curriculums. Sie schafft die Verbindung zwischen konzeptionellem Anspruch, didaktischer Umsetzung und konkreter Durchführung in der militärischen Ausbildungspraxis. Aus curricular-didaktischer Perspektive erfüllen die Module mehrere Funktionen zugleich. Sie strukturieren den Kompetenzaufbau in nachvollziehbare Entwicklungsstufen, ermöglichen die Verknüpfung von Grundlagenvermittlung, Spezialisierung und integrativer Anwendungsleistung und schaffen zugleich die Voraussetzung für Planbarkeit, Vergleichbarkeit und Qualitätssicherung. Gerade im Bereich militärischer SOC- und NOC-Ausbildung ist dies von besonderer Bedeutung, da hier nicht allein fachliches Wissen, sondern vor allem belastbare Handlungsfähigkeit unter realitätsnahen Bedingungen aufgebaut werden muss. Die Module sind daher nicht als isolierte Unterrichtsblöcke zu verstehen, sondern als aufeinander bezogene Bestandteile eines kohärenten Qualifizierungssystems, das individuelle Kompetenzentwicklung mit team- und organisationsbezogener Einsatzfähigkeit verbindet.

Die nachfolgende Modularchitektur folgt diesem Grundverständnis. Das Basismodul schafft ein gemeinsames fachliches, begriffliches und prozessuales Fundament für alle Teilnehmenden. Die darauf aufbauenden SOC- und NOC-Module vertiefen jene Kompetenzen, die für detektions- und analyseorientierte beziehungsweise betriebs- und netzwerkorientierte Rollen erforderlich sind. Die Abschlussübungen und Prüfungen führen diese Kompetenzen schließlich in einer integrativen, simulationsgestützten Umgebung zusammen und machen sichtbar, ob das im Curriculum angelegte Lernziel einer realitätsnahen und organisationswirksamen Handlungskompetenz erreicht wurde. Auf diese Weise bilden die Ausbildungsmodule das zentrale Bindeglied zwischen Wissensordnung, Rollenprofilen und praktischer Befähigung im Cyber- und Informationsraum.

5.8.1 Basismodul

Das Basismodul dient dem Aufbau eines gemeinsamen fachlichen, begrifflichen und prozessualen Fundaments für alle weiteren Ausbildungsanteile des Curriculums. Es richtet sich an sämtliche Teilnehmenden, unabhängig davon, ob sie im späteren Verlauf primär im Security Operations Center (SOC), im Network Operations Center (NOC) oder in angrenzenden Unterstützungs-, Führungs- oder Koordinationsfunktionen eingesetzt werden. Seine zentrale Funktion besteht darin, ein gemeinsames Ausgangsniveau herzustellen, auf dem spätere Spezialisierungen fachlich, organisatorisch und didaktisch belastbar aufbauen können. In curricularer Perspektive erfüllt das Basismodul damit eine strukturtragende Aufgabe: Es verhindert, dass weiterführende Ausbildungsphasen auf heterogenen Vorverständnissen, uneinheitlicher Begriffsverwendung oder nur implizit vorhandenen Deutungsmustern beruhen, die spätere Zusammenarbeit erschweren oder fachliche Vertiefung verzerren würden. Das Modul ist somit nicht lediglich ein vorbereitender Einstieg, sondern die erste verbindliche Stufe professioneller Cyber- und Netzbetriebsqualifizierung.

Inhaltlich werden im Basismodul jene Konzepte eingeführt, ohne die weder wirksame Detektion noch belastbarer Betrieb oder fundierte Reaktion möglich wären. Dazu zählen insbesondere Sicherheitsziele, Rollen und Verantwortlichkeiten, Identitäten und Berechtigungen, Schutzbedarfe, Klassifikation, Grundlagen von Risiko und Resilienz, Governance, Richtlinienarbeit, Awareness, Meldewege sowie der militärische Kontext von Cyber- und Informationsoperationen. Diese Inhalte

sind nicht als bloße Vorbemerkungen oder administrative Randthemen zu verstehen. Vielmehr definieren sie den begrifflichen, normativen und handlungspraktischen Rahmen, innerhalb dessen spezialisierte Tätigkeiten im SOC- und NOC-Bereich später sachgerecht ausgeführt werden können. Das Basismodul vermittelt daher nicht nur ein erstes Faktenwissen, sondern ein grundlegendes Verständnis dafür, wie technische, organisatorische, rechtliche und operationelle Dimensionen im Cyber- und Informationsraum miteinander verknüpft sind. In diesem Sinne zielt es darauf ab, ein gemeinsames professionelles Bezugssystem zu schaffen, das die spätere Ausbildung kohärent macht und zugleich die Anschlussfähigkeit zwischen unterschiedlichen Rollen und Funktionen erhöht.

Didaktisch ist das Basismodul als Orientierungs- und Fundamentierungsphase angelegt. Es kombiniert begriffliche Einführung, Fallbeispiele aus militärischen und kritischen Infrastrukturen, strukturierte Diskussionen, erste praktische Laboranteile und angeleitete Reflexionsphasen. Diese methodische Breite ist didaktisch deshalb sinnvoll, weil grundlegende Inhalte wie Identitätsmanagement, sichere Kommunikation, Risikoabschätzung oder Klassifikation in der Praxis häufig unterschätzt oder vorschnell als administrative Nebenaspekte wahrgenommen werden. Tatsächlich stellen sie jedoch operationelle Voraussetzungen für Handlungsfähigkeit dar. Wer etwa Schutzbedarfe nicht korrekt einschätzen kann, wird weder Prioritäten angemessen setzen noch wirksame Schutzmaßnahmen auswählen können. Wer Rollenverantwortung, Meldewege oder Grundprinzipien der Governance nicht versteht, wird auch bei ausgeprägter technischer Kompetenz Schwierigkeiten haben, sicherheitsrelevante Erkenntnisse organisatorisch wirksam werden zu lassen. Die didaktische Logik des Basismoduls besteht daher gerade darin, solche Grundlagen von Beginn an als handlungsrelevant und auftragsbezogen sichtbar zu machen. Das Basismodul darf deshalb nicht als bloßer „Vorkurs“ missverstanden werden, sondern ist als eigenständiger Qualifikationsbaustein zu begreifen, der zentrale professionelle Haltungen, Routinen und Deutungsmuster ausbildet. Gerade in militärischen Ausbildungsumgebungen ist dies von besonderer Bedeutung, da technisches Wissen, organisatorische Einbindung, rechtliche Vorgaben und Führungsbezug nicht getrennt nebeneinanderstehen, sondern ein zusammenhängendes professionelles Handlungsfeld bilden. Ein didaktisch tragfähiges Basismodul führt folglich nicht nur in Grundbegriffe ein, sondern vermittelt auch ein Verständnis dafür, wie technische Sachverhalte mit Auftrag, Verantwortung, Verfügbarkeit, Geheimschutz, Interoperabilität und legitimem Handeln zusammenhängen. Das Modul schafft damit die Voraussetzung dafür, dass die Teilnehmenden spätere Spezialisierungen nicht als isolierte technische Vertiefungen, sondern als funktional eingebettete Beiträge zur militärischen Handlungsfähigkeit begreifen. Ein zentrales Ziel des Basismoduls besteht in der Herstellung eines gemeinsamen Denk- und Sprachsystems. In komplexen militärischen Ausbildungs- und Einsatzkontexten ist eine einheitliche Terminologie keine formale Nebensache, sondern eine wesentliche Voraussetzung für Kooperation, Lageverständnis und konsistente Entscheidungsfindung. Missverständnisse zwischen technischen und nichttechnischen Akteuren, zwischen Spezialisten und Führungspersonal oder zwischen unterschiedlichen organisatorischen Teilbereichen entstehen häufig nicht aus mangelndem Engagement, sondern aus unterschiedlichen Begriffsverständnissen und abweichenden Deutungslogiken. Das Basismodul wirkt diesem Problem entgegen, indem es gemeinsame Begriffe, Konzepte und Bezugsrahmen etabliert, die über den weiteren Ausbildungsverlauf hinweg tragfähig bleiben. Dies ist organisationspraktisch besonders relevant, da sicherheitsrelevante Informationen im militärischen Kontext regelmäßig an Schnittstellen zwischen Fachpersonal, Führung, Stab, unterstützenden Stellen und angrenzenden Organisationseinheiten bearbeitet werden. Nur wenn Begriffe wie Risiko, Vorfall, Anomalie, Schutzbedarf, Eskalation oder Wiederherstellung in vergleichbarer Weise verstanden werden, kann ein belastbares gemeinsames Lage- und Handlungsverständnis entstehen.

Von besonderer Bedeutung ist dabei, dass Teilnehmende mit ausgeprägter technischer Vorerfahrung im Basismodul ein stärkeres Verständnis für rechtliche, organisatorische und führungsbezogene Aspekte entwickeln, während Teilnehmende mit eher operativer, administrativer oder koordinativer Prägung ein belastbares Fundament technischer Grundbegriffe erhalten. Das Modul schafft damit eine Brücke zwischen unterschiedlichen Vorwissenslagen und professionellen Perspektiven. Sein Ziel ist nicht die vollständige Angleichung aller Teilnehmenden, sondern ihre gegenseitige Anschlussfähigkeit. Gerade diese Anschlussfähigkeit ist für die spätere Zusammenarbeit in SOC- und NOC-nahen Strukturen von hoher Relevanz, weil militärische Wirksamkeit in diesem Bereich nicht aus homogener Expertise entsteht, sondern aus der koordinierten Zusammenarbeit unterschiedlicher Rollen und Fähigkeitsprofile. Ein wesentliches Ergebnis des Basismoduls ist die Herstellung von Anschlussfähigkeit für alle weiteren Ausbildungsanteile. Die Teilnehmenden sollen nach Abschluss in der Lage sein, sicherheitsrelevante Sachverhalte begrifflich korrekt zu erfassen, ihre Relevanz für den militärischen Auftrag zu beurteilen und sich in standardisierte Arbeits-, Melde- und Unterstützungsprozesse einzubringen. Sie sollen Grundmuster von Angriffen und Störungen erkennen, typische Verwundbarkeiten benennen, Risiken in ihrem jeweiligen Verantwortungsbereich nachvollziehbar beschreiben und einfache Schutz- oder Unterstützungsmaßnahmen begründet auswählen können. Damit bewegt sich das Basismodul an der Schwelle zwischen allgemeiner Sensibilisierung und professioneller Funktionsausbildung. Es vermittelt nicht nur Orientierungswissen, sondern erste handlungsrelevante Fähigkeiten, die als Voraussetzung für spätere Vertiefungen dienen. Zugleich sollen die Teilnehmenden verstehen, dass Cyber-Sicherheit im militärischen Kontext stets in Beziehung zu Führung, Verfügbarkeit, Geheimschutz, Interoperabilität und legitimem Handeln steht. Dieses Verständnis ist deshalb von zentraler Bedeutung, weil Cyber-Sicherheit im militärischen Bereich nicht als isolierter technischer Zweck, sondern als funktionaler Bestandteil übergreifender Einsatz- und Führungsfähigkeit begriffen werden muss.

Aus struktureller Sicht schafft das Basismodul damit die Voraussetzung für differenzierte Lernpfade im weiteren Curriculum. Erst auf der Grundlage eines gemeinsamen Fundaments kann zwischen SOC- und NOC-spezifischen Vertiefungen sinnvoll unterschieden werden, ohne dass diese Spezialisierungen in voneinander getrennte oder inkompatible Teilkulturen auseinanderlaufen. Das Basismodul stabilisiert das Curriculum somit nach unten, vereinheitlicht den Einstieg und reduziert das Risiko, dass fortgeschrittene Module durch stark unterschiedliche Vorkenntnisse ungleich wirksam werden. Es besitzt daher nicht nur eine vorbereitende, sondern auch eine ordnende und vereinheitlichende Funktion innerhalb der Gesamtarchitektur des Curriculums. Darüber hinaus kann das Basismodul in praktischer Hinsicht auch als Diagnoseinstrument für die weitere Ausbildung dienen. Durch kurze Eingangstests, Beobachtungen in ersten Übungssequenzen und die Auswertung von Fallbearbeitungen lassen sich Stärken, Entwicklungsbedarfe und geeignete Vertiefungspfade identifizieren. Dies ist didaktisch ebenso bedeutsam wie organisationspraktisch. Einerseits kann dadurch der weitere Lernprozess besser auf vorhandene Kompetenzen abgestimmt werden. Andererseits wird verhindert, dass spätere Spezialisierungen schematisch oder ausschließlich nach Verfügbarkeit vergeben werden. Stattdessen kann die weitere Ausbildung stärker kompetenzorientiert erfolgen. Diese diagnostische Funktion ist insbesondere vor dem Hintergrund moderner Workforce-Frameworks und proficiency-orientierter Ausbildungslogiken relevant, die professionelle Entwicklung nicht allein über formale Rollenbezeichnungen, sondern über nachvollziehbar definierte Kompetenzstände und Fähigkeitsprofile beschreiben [138], [140]. Das Basismodul liefert hierfür eine erste belastbare Grundlage und unterstützt damit nicht nur den individuellen Einstieg in das Curriculum, sondern auch dessen qualitätsgesicherte Steuerung und die differenzierte Personalentwicklung.

5.8.2 SOC Modul

Das SOC-Modul vertieft jene Fähigkeiten, die für die Erkennung, Analyse, Bewertung und koordinierte Reaktion auf sicherheitsrelevante Ereignisse in militärischen Informations- und Kommunikationsumgebungen erforderlich sind. Es baut auf dem im Basismodul hergestellten gemeinsamen fachlichen, begrifflichen und prozessualen Fundament auf und überführt dieses in einen detektions- und analyseorientierten Spezialisierungsstrang. Inhaltlicher Schwerpunkt sind die Kernfunktionen eines militärischen Security Operations Center: die Sammlung, Sichtung und Korrelation sicherheitsrelevanter Ereignisdaten, die Bildung und Prüfung analytischer Hypothesen, die Validierung und Priorisierung von Alarmen, die Einordnung von Anomalien, die Nutzung von Threat-Intelligence-Informationen, forensische Vertiefungsschritte, die Verdichtung technischer Beobachtungen zu einem belastbaren Lagebild sowie die Vorbereitung fachlich fundierter Handlungsoptionen für Führungs- und Entscheidungsprozesse. Das Modul ist damit auf jene Aufgaben ausgerichtet, bei denen technische Beobachtung in operationelle Bedeutung übersetzt werden muss. Seine besondere Relevanz liegt darin, dass im militärischen Kontext nicht die bloße Feststellung eines sicherheitsrelevanten Ereignisses ausreicht, sondern dessen Bedeutung für Auftrag, Schutzgüter, Kommunikationsfähigkeit, Führungsfähigkeit und potenzielle Folgewirkungen bewertet werden muss.

Didaktisch steht im SOC-Modul die Entwicklung analytischer Urteilkraft im Vordergrund. Die Teilnehmenden sollen lernen, auch unter Bedingungen von Unsicherheit, Zeitdruck und unvollständiger Informationslage zwischen bloßem Datenrauschen und tatsächlich relevanten Indikatoren zu unterscheiden, Einzelsignale in übergeordnete Angriffsmuster einzuordnen, konkurrierende Hypothesen gegeneinander abzuwägen und daraus priorisierte Maßnahmen abzuleiten. Diese Zielsetzung ist aus curriculardidaktischer Sicht besonders bedeutsam, weil professionelle Tätigkeit im SOC nicht auf das Bedienen einzelner Werkzeuge oder das Abarbeiten vordefinierter Routinen reduziert werden kann. Vielmehr verlangt sie die Fähigkeit, Beobachtungen methodisch einzuordnen, Unsicherheit zu explizieren und technische Befunde so aufzubereiten, dass daraus handlungsrelevante Erkenntnisse entstehen. Anders als in rein toolzentrierten Trainings wird das Arbeiten mit SIEM-Systemen, Sensorik, Telemetrie, Log-Daten und Threat-Intelligence-Quellen deshalb nicht als Selbstzweck vermittelt. Werkzeuge werden im Rahmen des Moduls als Mittel der Erkenntnisgewinnung, der strukturierten Kommunikation und der Entscheidungsunterstützung verstanden. Diese Perspektive ist im militärischen Umfeld von besonderer Bedeutung, weil technische Befunde nur dann wirksam werden, wenn sie in eine nachvollziehbare Lageeinschätzung und in adressatengerechte Reaktionsoptionen übersetzt werden. Das SOC-Modul vermittelt daher nicht nur technische Analysefähigkeiten, sondern fördert auch die Kompetenz, sicherheitsrelevante Ereignisse hinsichtlich ihrer operativen Tragweite zu bewerten. Die Teilnehmenden sollen in die Lage versetzt werden, nicht nur zu erkennen, dass ein Vorfall vorliegt, sondern auch einzuschätzen, welche Systeme betroffen sind, welche unmittelbaren und mittelbaren Auswirkungen auf Kommunikationsbeziehungen, Führungsunterstützung, Aufklärungsfähigkeit oder missionskritische Dienste möglich sind und welche Unsicherheiten in der Bewertung bestehen bleiben. Ebenso gehört dazu, zu unterscheiden, welche Maßnahmen sofort einzuleiten sind, welche vorbereitend geplant werden sollten und welche aufgrund ihrer Tragweite oder Wirkung genehmigungs- oder abstimmungspflichtig sind. In dieser Perspektive ist das SOC-Modul nicht lediglich ein Analysemodul, sondern ein Modul zur militärischen Entscheidungsunterstützung im Cyber- und Informationsraum. Es verbindet die technische Dimension der Detektion mit der organisatorischen und führungsbezogenen Dimension von Lagebewertung, Meldung, Eskalation und verantworteter Reaktion.

Ein besonderer Schwerpunkt des Moduls liegt auf der Schnittstelle zwischen SOC, NOC, Führung und weiteren unterstützenden Stellen. In realen militärischen Lagen ist ein SOC nicht als isolierte Fachinstanz wirksam, sondern als Knotenpunkt innerhalb eines arbeitsteiligen Systems, in dem

Informationen erhoben, bewertet, verdichtet und weitergegeben werden müssen. Daraus ergibt sich die Notwendigkeit, technische Erkenntnisse nicht nur fachlich korrekt, sondern auch adressatengerecht zu kommunizieren. Die Teilnehmenden müssen daher lernen, komplexe oder unsichere Befunde so darzustellen, dass sie für andere Rollen und Ebenen handlungsrelevant werden. Dies betrifft insbesondere die Verdichtung von Unsicherheit, die Formulierung belastbarer Lageeinschätzungen, die Unterscheidung zwischen bestätigten und vermuteten Befunden sowie die nachvollziehbare Begründung von Prioritäten und Handlungsempfehlungen. Professionelle SOC-Arbeit ist insofern immer auch Kommunikationsarbeit. Sie verlangt die Fähigkeit, technische Tiefe mit strukturiertem Lageverstehen und organisationsbezogener Anschlussfähigkeit zu verbinden.

Methodisch eignet sich für dieses Modul eine Kombination aus szenariobasierten Lagebildern, forensisch angeleiteten Fallbearbeitungen, Alarm-Triage in Echtzeit, Tabletop-Übungen, simulationsgestützten Cyber-Range-Sequenzen und strukturierten Debriefings. Diese Formate sind didaktisch deshalb besonders geeignet, weil sie die eigentliche Komplexität der SOC-Tätigkeit sichtbar machen. Sie zeigen, dass sich professionelle Analyse nicht in der Einzelarbeit an Daten oder Werkzeugen erschöpft, sondern in einem Zusammenspiel aus Hypothesenbildung, Kommunikation, Teamkoordination, Eskalationsentscheidungen, Dokumentation und zeitkritischer Bewertung vollzieht. Gerade strukturierte Debriefings besitzen hierbei eine hohe Bedeutung, weil sie ermöglichen, analytische Denkwege, Fehleinschätzungen, Priorisierungsprobleme und gelungene Entscheidungsprozesse im Nachgang nachvollziehbar zu machen. Auf diese Weise fördert das Modul nicht nur die unmittelbare Leistungsfähigkeit, sondern auch die Reflexionsfähigkeit der Teilnehmenden. Reflexion ist in diesem Zusammenhang kein bloßes pädagogisches Zusatzmoment, sondern ein Bestandteil professioneller Entwicklung, weil analytische Qualität im Cyber- und Informationsraum wesentlich davon abhängt, wie aus Erfahrung, Rückmeldung und strukturiertem Nachdenken gelernt wird. Ausbildungssystematisch bildet das SOC-Modul den detektions- und analyseorientierten Spezialisierungsstrang des Curriculums. Es soll die Teilnehmenden dazu befähigen, von einer reaktiven Bearbeitung einzelner Alarmmeldungen zu einer proaktiven, lageorientierten und methodisch nachvollziehbaren Sicherheitsanalyse überzugehen. Diese Verschiebung ist von zentraler Bedeutung, weil ein leistungsfähiges militärisches SOC nicht nur auf bereits manifest gewordene Vorfälle reagieren, sondern Entwicklungen frühzeitig erkennen, Muster identifizieren und Handlungsfenster sichtbar machen muss. Dadurch erhöht sich nicht nur die Wahrscheinlichkeit früher Erkennung, sondern auch die Qualität der Maßnahmen, die in der Folge durch NOC, Stab, Führung oder weitere Fachstellen umgesetzt, abgestimmt oder freigegeben werden. Das Modul trägt damit unmittelbar zur Verbesserung der Reaktionsfähigkeit, der Lagequalität und der Kohärenz militärischer Entscheidungsprozesse im Cyber- und Informationsraum bei. Darüber hinaus unterstützt das SOC-Modul eine rollenbasierte Professionalisierung im Sinne moderner Cyber-Workforce-Modelle. Die konsequente Zuordnung von Aufgaben, Kenntnissen, Fertigkeiten und Verantwortungsniveaus erleichtert es, Ausbildungsstände transparent zu machen und Personal gezielt weiterzuentwickeln [138], [139]. Für militärische Organisationen ist dies von besonderer Relevanz, weil personelle Rotation, Schichtbetrieb und unterschiedliche Vorverwendungen nur dann beherrschbar bleiben, wenn SOC-Kompetenz systematisch beschrieben, geprüft und nachentwickelt werden kann. Das Modul schafft hierfür eine belastbare Grundlage, indem es analytische, kommunikative und organisationsbezogene Anforderungen nicht voneinander trennt, sondern als zusammengehörige Bestandteile professioneller Rollenbefähigung behandelt. Es trägt damit nicht nur zur individuellen Qualifizierung, sondern auch zur institutionellen Stabilisierung von SOC-Fähigkeiten bei.

5.8.3 NOC Modul

Das NOC-Modul vertieft jene Kompetenzen, die für den sicheren, stabilen und resilienten Betrieb militärischer Kommunikations- und Netzwerkinfrastrukturen erforderlich sind. Es baut auf dem im

Basismodul geschaffenen gemeinsamen fachlichen, begrifflichen und prozessualen Fundament auf und bildet innerhalb des Curriculums den betriebs- und netzwerkorientierten Spezialisierungsstrang. Während das SOC-Modul seinen Schwerpunkt auf Detektion, Analyse und Lageverdichtung legt, richtet das NOC-Modul den Blick stärker auf Verfügbarkeit, Stabilität, Performance, Segmentierung, Wiederherstellung und die operative Beherrschung komplexer Netz- und Verbundsysteme. Dies schließt die Analyse von Netzwerkverkehr, die Überwachung von Diensten, die Erkennung betriebsnaher Anomalien, den Umgang mit Fehlfunktionen, die Bewertung von Architekturabhängigkeiten sowie den Schutz und Betrieb OT-naher oder cyber-physischer Teilumgebungen ein. Im militärischen Kontext ist diese Perspektive von besonderer Bedeutung, weil die Wirksamkeit zahlreicher Führungs-, Aufklärungs- und Einsatzsysteme unmittelbar von der verlässlichen Funktion des zugrunde liegenden Netzes abhängt. Das NOC-Modul thematisiert Betrieb daher nicht als rein technischen Hintergrundprozess, sondern als zentrale Voraussetzung militärischer Führungs- und Einsatzfähigkeit.

Didaktisch verfolgt das Modul das Ziel, betriebliche Urteilskraft und technische Handlungsfähigkeit unter belastungsnahen Bedingungen aufzubauen. Die Teilnehmenden sollen verstehen, wie sich sicherheitsrelevante Ereignisse, Fehlkonfigurationen, Lastspitzen, Segmentausfälle oder OT-bezogene Besonderheiten auf Dienste, Verbundsysteme und Kommunikationswege auswirken. Damit geht das Modul deutlich über die rein formale Überwachung technischer Parameter hinaus. Es qualifiziert dazu, Netzwerkzustände nicht nur zu beobachten, sondern ihre Bedeutung für den militärischen Auftrag, für die Kontinuität der Leistungserbringung und für die Stabilität missionskritischer Prozesse zu interpretieren. Diese Ausrichtung ist curriculardidaktisch bedeutsam, weil professionelle NOC-Arbeit nicht in der isolierten Beherrschung einzelner Technologien besteht, sondern in der Fähigkeit, technische Zusammenhänge in ihrer operativen Relevanz zu verstehen und daraus sachgerechte Entscheidungen oder Empfehlungen abzuleiten. Ein zentrales Merkmal des NOC-Moduls besteht in der Verbindung von klassischem Betriebswissen mit der Logik von Cyber-Sicherheit und Resilienz. Verfügbarkeit wird dabei nicht gegen Sicherheit ausgespielt, sondern als integraler Bestandteil einer widerstandsfähigen Sicherheitsarchitektur verstanden. Gerade in militärischen Netzen und OT-nahen Umgebungen ist diese Integration entscheidend, weil Schutzmaßnahmen nur dann wirksam und legitim sind, wenn sie den betrieblichen Auftrag nicht unbeabsichtigt unterlaufen. Das Modul vermittelt daher ein Verständnis dafür, dass sichere und resiliente Betriebsführung nicht allein darin besteht, Ausfälle zu vermeiden, sondern darin, Systeme auch unter widrigen Bedingungen kontrolliert weiterzubetreiben, degradierte Betriebsarten vorzubereiten und Wiederherstellungsmaßnahmen so zu priorisieren, dass operative Handlungsfähigkeit möglichst erhalten bleibt. Damit wird deutlich, dass Betriebssicherheit, Cyber-Sicherheit und militärische Auftragserfüllung nicht als getrennte Ziele zu begreifen sind, sondern in einem wechselseitigen Funktionszusammenhang stehen.

Ein besonderer Schwerpunkt des NOC-Moduls liegt auf Abhängigkeiten, Kritikalitäten und Wiederherstellungslogiken. Die Teilnehmenden sollen nachvollziehen können, welche Dienste, Pfade, Segmente, Komponenten und externen Schnittstellen für die Aufrechterhaltung wesentlicher Fähigkeiten kritisch sind und wie sich Störungen in einem Teilbereich auf andere Bereiche auswirken können. Dieses Denken in Abhängigkeiten ist im militärischen Kontext unverzichtbar, weil komplexe Netz- und Verbundsysteme selten isoliert betrieben werden, sondern in vielfacher Weise miteinander gekoppelt sind. Eine Störung in einem Segment kann daher weitreichende Folgeeffekte für Kommunikation, Führungsunterstützung, Datenverfügbarkeit oder Synchronisationsprozesse haben. Das NOC-Modul zielt darauf ab, solche Zusammenhänge nicht erst im akuten Störfall zu erkennen, sondern bereits im Vorfeld systematisch zu analysieren und in Wiederherstellungs- und Degradationsplanungen zu berücksichtigen. Die Teilnehmenden sollen in die Lage versetzt werden, Prioritäten für Wiederanlauf und Umkonfiguration festzulegen, betriebliche Ausweichoptionen vorzubereiten und im Störfall zwischen sicherheitstechnisch gebotenen, operativ vertretbaren und ressourcenmäßig realisierbaren Maßnahmen abzuwägen.

Gerade diese Fähigkeit zur kontrollierten Degradation und nachvollziehbaren Wiederherstellung ist für militärische Organisationen von hoher Relevanz. Das Modul qualifiziert daher nicht nur für den Routinebetrieb, sondern ausdrücklich auch für Situationen, in denen der Betrieb unter Störung, Angriff, Ressourcenknappheit oder eingeschränkter Führbarkeit fortgeführt werden muss. In diesem Sinn trägt das NOC-Modul unmittelbar zur praktischen Umsetzung des im Curriculum verankerten Resilienz- und „fight through“-Gedankens bei. Resilienz wird dabei nicht als abstrakter Leitbegriff behandelt, sondern als konkrete betriebliche Fähigkeit, auch unter verschlechterten Bedingungen handlungsfähig zu bleiben, Prioritäten neu zu ordnen und technische Stabilität mit operativer Zweckmäßigkeit zu verbinden. Ein robustes NOC ist daher nicht nur für Normalzustände zuständig, sondern insbesondere für jene Situationen, in denen Systeme nicht mehr ideal funktionieren und dennoch funktionsfähig gehalten, umkonfiguriert oder schrittweise wiederhergestellt werden müssen.

Methodisch eignet sich für dieses Modul eine Kombination aus topologiebezogenen Laborübungen, Traffic-Analysen, Segmentierungs- und Wiederanlauf-Szenarien, OT-nahen Fallstudien, Störungsdiagnosen unter Zeitdruck sowie gekoppelten Übungsformaten mit SOC- und Stabsanteilen. Diese Formate sind didaktisch besonders geeignet, weil sie die eigentliche Komplexität betriebsnaher Entscheidungen sichtbar machen. Sie zeigen, dass NOC-Arbeit nicht im bloßen Abarbeiten technischer Checklisten besteht, sondern in der fortlaufenden Bewertung von Zuständen, Auswirkungen, Abhängigkeiten und Handlungsoptionen. Gerade Zeitdruckübungen und gekoppelte Szenarien machen deutlich, dass betriebliche Entscheidungen selten rein technisch sind, sondern fast immer sicherheitsbezogene, organisatorische und operative Implikationen besitzen. Strukturierte Debriefings sind auch hier von besonderer Bedeutung, weil sie helfen, Fehlannahmen, Kommunikationsprobleme, Priorisierungsfehler und gelungene Reaktionsmuster im Nachgang sichtbar zu machen. Auf diese Weise wird das Modul nicht nur zum Ort unmittelbaren Kompetenzerwerbs, sondern auch zu einem Raum reflektierter professioneller Entwicklung. Eine besondere Rolle spielt im NOC-Modul die Ausbildung von Schnittstellenkompetenz. Teilnehmende müssen lernen, Betriebsrisiken klar zu beschreiben, Auswirkungen auf missionskritische Dienste nachvollziehbar zu erläutern und die Konsequenzen verschiedener Handlungsoptionen transparent zu machen. Dies betrifft insbesondere die Kommunikation an den Schnittstellen zu SOC, OT-Verantwortlichen, Führungsunterstützung und Stab. Gerade in militärischen Kontexten ist ein NOC nicht lediglich technischer Betreiber, sondern Teil eines arbeitsteiligen Systems, in dem Informationen, Bewertungen und Entscheidungen zwischen mehreren Ebenen und Funktionen koordiniert werden müssen. Professionelle NOC-Arbeit verlangt deshalb nicht nur technische Tiefe, sondern auch die Fähigkeit, betriebliche Sachverhalte so zu übersetzen, dass sie für andere Rollen handlungsrelevant werden. Wer etwa degradierte Betriebsarten vorbereitet oder Wiederherstellungsprioritäten festlegt, muss deren Folgen für Lagebild, Auftragserfüllung und Führungsfähigkeit adressatengerecht kommunizieren können. Das Modul stärkt damit nicht nur technische Betriebskompetenz, sondern auch organisationsbezogene Kommunikations- und Koordinationsfähigkeit.

Ausbildungssystematisch bildet das NOC-Modul den betriebs- und netzwerkorientierten Spezialisierungsstrang des Curriculums. Es stärkt jene Fähigkeiten, die in vielen Organisationen unterschätzt werden: Cyberverteidigung ist nicht nur eine Frage der Erkennung und Analyse von Angriffen, sondern in gleichem Maß eine Frage des robusten Betriebs, der kontrollierten Degradation und der nachvollziehbaren Wiederherstellung. Indem das NOC-Modul diese Perspektive systematisch ausbildet, erhöht es die Resilienz der gesamten Organisationsarchitektur und verbessert die Anschlussfähigkeit zwischen technischem Betrieb, Sicherheitsanalyse und militärischer Führung. Es trägt dazu bei, dass Störungen und Angriffe nicht nur erkannt, sondern auch in ihrer betrieblichen Tragweite verstanden und in wirksame Maßnahmen zur Stabilisierung und Wiederherstellung überführt werden können. Darüber hinaus unterstützt das NOC-Modul eine rollenbasierte Professionalisierung im Sinne moderner Kompetenz- und Workforce-Modelle. Die

systematische Zuordnung von Aufgaben, Kenntnissen, Fertigkeiten und Verantwortungsniveaus erleichtert es, Ausbildungsstände transparent zu machen und Personal gezielt weiterzuentwickeln. Für militärische Organisationen ist dies besonders bedeutsam, weil personelle Rotation, unterschiedliche Vorverwendungen, begrenzte Spezialressourcen und der Bedarf an durchhaltefähigem Schichtbetrieb nur dann beherrschbar bleiben, wenn NOC-Kompetenzen systematisch beschrieben, überprüft und nachentwickelt werden können. Das Modul schafft hierfür eine belastbare Grundlage, indem es technische, betriebliche und kommunikative Anforderungen nicht als getrennte Elemente behandelt, sondern als zusammengehörige Bestandteile professioneller Rollenbefähigung versteht.

5.8.4 Abschlussübungen und Prüfungen

Die Abschlussübungen und Prüfungen haben die Funktion, die im Verlauf des Curriculums aufgebauten Kenntnisse, Fertigkeiten und professionellen Haltungen in realitätsnahen Gesamtlagen zusammenzuführen, sichtbar zu machen und überprüfbar zu bewerten. Sie markieren damit nicht lediglich das Ende eines Ausbildungsabschnitts, sondern bilden den curricularen Ort, an dem sich zeigt, ob aus einzelnen Wissensbeständen tatsächlich belastbare Handlungskompetenz geworden ist. In militärischen SOC- und NOC-Kontexten ist dies von besonderer Bedeutung, weil operationelle Wirksamkeit nur in begrenztem Maß durch isolierte Wissensabfragen erfasst werden kann. Entscheidend ist vielmehr, ob Teilnehmende in komplexen, dynamischen und arbeitsteiligen Situationen in der Lage sind, Informationen zu priorisieren, Unsicherheit zu kommunizieren, Maßnahmen abzustimmen und unter Einhaltung rechtlicher, organisatorischer und ethischer Vorgaben handlungsfähig zu bleiben. Die Abschlussphase ist daher nicht bloß ein Prüfungsformat im engen Sinn, sondern ein integraler Bestandteil kompetenzorientierter Ausbildung.

Für die vorliegende Curriculumsarchitektur ist dabei wesentlich, dass die integrativen Übungen und anwendungsorientierten Prüfungsanteile konsequent in einem Cyber Lab beziehungsweise einer Cyber Range durchgeführt werden. Diese Lernumgebung ist didaktisch besonders geeignet, weil sie eine kontrollierte, technisch realitätsnahe und zugleich pädagogisch gestaltbare Simulationsumgebung bereitstellt, in der komplexe Sicherheits-, Betriebs- und Störungsszenarien abgebildet werden können, ohne operative Echtumgebungen zu gefährden. Ein Cyber Lab oder eine Cyber Range ermöglicht es, Ereignisse, Abhängigkeiten, Eskalationen und Auswirkungen in einer Form nachzustellen, die für die Lernenden handlungspraktisch erfahrbar wird. Damit wird ein Ausbildungsraum geschaffen, in dem nicht nur technisches Detailwissen geprüft, sondern vor allem die Fähigkeit zur Lageerfassung, Lagebewertung, teambezogenen Koordination und rollenadäquaten Entscheidungsunterstützung unter realitätsnahen Bedingungen beobachtet werden kann. Gerade im militärischen Kontext ist dies von hoher Relevanz, weil hier Ausbildung nicht auf abstrakte Wissensvermittlung begrenzt bleiben darf, sondern auf belastbare Handlungsfähigkeit in komplexen technischen und organisatorischen Lagen zielen muss.

Die Abschlussphase sollte daher mehrstufig und methodisch differenziert angelegt sein. Sie umfasst erstens wissens- und verständnisbezogene Prüfungsanteile, mit denen zentrale Konzepte, Begriffe, Verfahren und Rahmenbedingungen verlässlich überprüft werden. Diese Formate behalten ihre Berechtigung, weil professionelles Handeln auch auf einem belastbaren begrifflichen und methodischen Fundament beruhen muss. Zweitens umfasst die Abschlussphase anwendungsorientierte Leistungsnachweise, die im Cyber Lab oder in der Cyber Range durchgeführt werden und in denen Analyse, Betrieb, Eskalation, Dokumentation und Lagekommunikation in simulierter Echtzeit beobachtet werden können. Drittens sollten integrierte Teamübungen vorgesehen werden, in denen das Zusammenwirken von SOC, NOC, OT-nahen Rollen und – soweit organisatorisch möglich – Führungs- oder Stabsanteilen abgebildet wird. Diese Staffelung ist didaktisch sinnvoll, weil unterschiedliche Kompetenzdimensionen nur in

unterschiedlichen Formaten sichtbar werden. Reproduktives Wissen kann schriftlich oder mündlich überprüft werden, während kooperative Handlungskompetenz, professionelle Kommunikation und belastbare Lagebeurteilung erst in simulationsgestützten und teambezogenen Szenarien sichtbar werden. Die besondere Stärke der Cyber Range als Prüfungs- und Übungsraum liegt darin, dass sie die Verschränkung von technischer Komplexität und organisatorischer Handlungsanforderung abbilden kann. In einer solchen Umgebung lassen sich sicherheitsrelevante Ereignisse, Netzwerkstörungen, Fehlkonfigurationen, Angriffsverläufe, Kommunikationsunterbrechungen, Eskalationsdynamiken und Wiederherstellungsanforderungen in abgestufter Schwierigkeit simulieren. Dadurch können die Teilnehmenden nicht nur zeigen, dass sie einzelne Verfahren beherrschen, sondern dass sie diese Verfahren unter Zeitdruck, mit unvollständiger Informationslage und in Koordination mit anderen Rollen anwenden können. Für SOC-Personal bedeutet dies insbesondere, dass Alarmvalidierung, Hypothesenbildung, Korrelation, Lageverdichtung und Eskalation unter realitätsnahen Bedingungen erprobt werden. Für NOC-Personal wird sichtbar, ob Störungen, Abhängigkeiten, degradierte Betriebszustände und Wiederherstellungsoptionen technisch korrekt und zugleich auftragsbezogen bewertet werden können. Für beide Rollen zusammen eröffnet die Cyber Range die Möglichkeit, Schnittstellenarbeit, Kommunikationsqualität und Übergänge zwischen Analyse, Betrieb und Führungsunterstützung konkret zu beobachten. Ein weiterer didaktischer Vorteil liegt darin, dass Cyber-Lab- und Cyber-Range-Umgebungen die graduelle Gestaltung von Komplexität erlauben. Szenarien können so aufgebaut werden, dass sie zunächst klar strukturierte Lagen mit begrenztem Variablenumfang darstellen und schrittweise zu mehrdeutigen, gekoppelten und dynamischen Gesamtsituationen erweitert werden. Auf diese Weise kann die Abschlussphase nicht nur als punktuelle Endprüfung verstanden werden, sondern auch als kontrollierte Verdichtung des gesamten Lernprozesses. Die Lernenden müssen dann nicht lediglich eine einzelne technische Aufgabe lösen, sondern in einer Gesamtlage zeigen, dass sie Beobachtungen einordnen, relevante von irrelevanten Informationen unterscheiden, begründete Entscheidungen treffen und diese adressatengerecht kommunizieren können. Dies ist im militärischen Ausbildungszusammenhang besonders bedeutsam, weil reale Lagen selten monokausal, vollständig transparent oder rein technisch lösbar sind. Die Cyber Range bildet damit einen Raum, in dem die Mehrdimensionalität von Handlungskompetenz tatsächlich geprüft werden kann.

Für die Bewertung der Abschlussphase empfiehlt sich ein kombiniertes Modell aus kriterialen Bewertungsrastern, beobachtbarem Rollenverhalten, Ergebnisqualität und Reflexionsleistung. Bewertet werden sollten unter anderem die Qualität der Lageerfassung, die Plausibilität von Hypothesen, die Nachvollziehbarkeit von Priorisierungsentscheidungen, der Umgang mit Unsicherheit, die Adressatengerechtigkeit von Meldungen, die Qualität der Teamkoordination, die Fähigkeit zur Einhaltung definierter Playbooks oder Eskalationswege sowie die begründete Berücksichtigung rechtlicher und ethischer Rahmenbedingungen. In Cyber-Range-Szenarien kann darüber hinaus beobachtet werden, wie Teilnehmende unter Belastung mit Zeitdruck, Störungen, widersprüchlichen Informationen oder Rollenunklarheit umgehen. Ein solcher Bewertungsansatz ist mit kompetenzorientierten Workforce- und Proficiency-Modellen gut vereinbar, weil er nicht nur „Wissen über“ ein Thema, sondern demonstrierte Befähigung im Handlungskontext in den Mittelpunkt stellt [138], [140]. Gerade in militärischen Ausbildungsumgebungen ist dies wesentlich, da dort nicht allein Fachrichtigkeit, sondern auch Verantwortungsfähigkeit, Kommunikationsleistung, Teamorientierung und Anschlussfähigkeit an organisationale Prozesse geprüft werden müssen. Besondere Bedeutung kommt in diesem Zusammenhang dem Debriefing zu, das im Anschluss an Cyber-Lab- oder Cyber-Range-Sequenzen erfolgen sollte. Die eigentliche Lertiefe vieler Abschlussübungen entsteht nicht nur im Handeln selbst, sondern in der strukturierten Auswertung des Handelns. Debriefings ermöglichen es, Entscheidungswege, Fehlannahmen, Kommunikationsprobleme, gelungene Koordinationsmuster und Priorisierungslogiken im Nachgang sichtbar zu machen. Die Teilnehmenden erhalten dadurch nicht nur eine Bewertung, sondern eine reflektierte Rückmeldung darüber, welche Annahmen tragfähig

waren, an welchen Stellen Unsicherheit unzureichend kommuniziert wurde, wo technische und organisatorische Aspekte nicht hinreichend verzahnt waren und welche alternativen Handlungsoptionen bestanden hätten. Gerade in der Cyber Range kann diese Rückmeldung besonders gehaltvoll sein, weil technische Prozessdaten, Kommunikationsverläufe, Zeitlinien und Reaktionsmuster systematisch rekonstruiert und in die Auswertung einbezogen werden können. Damit wird die Abschlussphase zugleich zu einem Raum vertieften Lernens und nicht nur zu einem Instrument selektiver Leistungsfeststellung.

Darüber hinaus erfüllen Abschlussübungen in der Cyber Range auch eine wichtige Funktion für das organisationale Lernen. Wenn Beobachtungen, Fehlerbilder, Kommunikationsprobleme, Entscheidungsengpässe und Stärken systematisch dokumentiert werden, liefern die Ergebnisse wertvolle Hinweise für die Weiterentwicklung von Modulen, Playbooks, Rollenprofilen und Führungsprozessen. In diesem Sinn sind Abschlussprüfungen nicht als isolierte Momentaufnahme individueller Leistung zu verstehen, sondern auch als Feedbackmechanismus für das Curriculum selbst. Sie machen sichtbar, an welchen Stellen Ausbildungsinhalte tragfähig sind, wo Übergänge zwischen Modulen verbessert werden müssen und welche Kompetenzen in künftigen Ausbildungsdurchgängen stärker vertieft werden sollten. Besonders in Cyber-Lab- und Cyber-Range-Umgebungen ist dieser Rückkopplungseffekt wertvoll, weil dort komplexe Szenarien standardisiert, wiederholt und vergleichbar durchgeführt werden können. Dies erhöht die Aussagekraft von Beobachtungen und unterstützt eine evidenzbasierte Weiterentwicklung der Ausbildung. Schließlich schaffen Abschlussübungen und Prüfungen Legitimität, Transparenz und Verlässlichkeit. Sie machen sichtbar, welches Kompetenzniveau mit welchem Ausbildungsabschnitt tatsächlich verbunden ist, und unterstützen damit Personalentwicklung, Einsatzplanung und Vertrauensbildung innerhalb der Organisation. Für militärische Entscheidungsträger ist dies von besonderer Bedeutung, weil nur belastbar qualifiziertes Personal in hochkritischen Cyber- und Netzwerkfunktionen eingesetzt werden sollte. Die im Cyber Lab beziehungsweise in der Cyber Range durchgeführten Abschlussübungen leisten daher einen doppelten Beitrag: Sie sichern Lernerfolg nach innen und Verlässlichkeit nach außen. Nach innen machen sie für Teilnehmende, Ausbildende und Vorgesetzte sichtbar, welche Kompetenzen aufgebaut wurden und wo weiterer Entwicklungsbedarf besteht. Nach außen schaffen sie eine nachvollziehbare Grundlage dafür, Ausbildungsstände, Rollenbefähigung und Einsatzreife transparent zu bewerten.

5.9 Qualitätssicherung und Weiterentwicklung

Die Entwicklung eines Curriculums für den militärischen Cyber- und Informationsraum kann nicht als abgeschlossener Einmalprozess verstanden werden, sondern erfordert eine kontinuierliche Überprüfung, Anpassung und fachliche Weiterentwicklung. Angesichts dynamischer Bedrohungslagen, technologischer Veränderungen sowie sich wandelnder organisationaler Anforderungen ist die langfristige Wirksamkeit eines Ausbildungsprogramms wesentlich davon abhängig, in welchem Ausmaß seine Inhalte, Formate und Zielsetzungen systematisch reflektiert und fortgeschrieben werden. Qualitätssicherung ist dabei nicht lediglich als nachgelagerte Kontrolle zu begreifen, sondern als integraler Bestandteil curricularer Steuerung und Professionalisierung. Das vorliegende Kapitel beschreibt daher jene Prinzipien, Verfahren und strukturellen Voraussetzungen, durch die die Qualität des Curriculums gesichert und seine Weiterentwicklung nachhaltig ermöglicht werden kann. Im Zentrum stehen dabei sowohl evaluative Rückkopplungsmechanismen als auch Prozesse der inhaltlichen Aktualisierung, institutionellen Verankerung und lernorientierten Anpassung. Qualitätssicherung und Weiterentwicklung werden damit als komplementäre Dimensionen eines Curriculums verstanden, das auf wissenschaftliche Fundierung, praktische Anschlussfähigkeit und langfristige Relevanz ausgerichtet ist.

5.9.1 Grundprinzipien der Qualitätssicherung

Die Qualitätssicherung des vorliegenden Curriculums beruht auf mehreren leitenden Grundprinzipien, die seine Planung, Durchführung, Evaluation und Weiterentwicklung bestimmen. Diese Grundprinzipien sind nicht als nachgelagerte Kontrollmechanismen zu verstehen, sondern als integraler Bestandteil curricularer Steuerung. In einem sicherheitskritischen und technologisch dynamischen Handlungsfeld wie dem militärischen Cyber- und Informationsraum kann ein Curriculum nur dann dauerhaft wirksam bleiben, wenn seine Ziele, Inhalte, Methoden und Leistungsnachweise regelmäßig auf Konsistenz, Relevanz und Wirkung überprüft werden. Qualitätssicherung ist in diesem Zusammenhang nicht auf die formale Bewertung einzelner Lehrveranstaltungen oder die Erhebung allgemeiner Zufriedenheit zu reduzieren. Sie zielt vielmehr darauf ab, die fachliche Belastbarkeit, didaktische Kohärenz und operationelle Brauchbarkeit des Curriculums dauerhaft sicherzustellen. Daraus ergeben sich mehrere Grundprinzipien, die gemeinsam den normativen und praktischen Rahmen der Qualitätssicherung bilden.

Ein erstes Grundprinzip ist das Prinzip der Integration. Qualitätssicherung ist nicht als externer Zusatz zur Ausbildung zu begreifen, sondern als inhärenter Bestandteil des Curriculums selbst. Sie beginnt bereits bei der Formulierung von Lernzielen, setzt sich in der Auswahl und Gewichtung von Wissensgebieten fort, prägt die Gestaltung von Modulen, Übungen und Prüfungen und wirkt bis in die Auswertung und Weiterentwicklung des Gesamtsystems hinein. In diesem Verständnis ist Qualitätssicherung keine abschließende Kontrolle dessen, was bereits entwickelt und durchgeführt wurde, sondern ein durchgängiges Steuerungsprinzip. Gerade in militärischen Ausbildungszusammenhängen ist diese Integration wesentlich, weil die Qualität von Ausbildung nicht erst am Ende in Prüfungen sichtbar wird, sondern bereits in der Kohärenz ihrer Zielarchitektur, in der methodischen Stringenz ihrer Durchführung und in ihrer Anschlussfähigkeit an reale Verwendungszusammenhänge angelegt ist.

Ein zweites Grundprinzip ist das Prinzip der Kohärenz. Lernziele, Wissensgebiete, Module, Übungsformen und Leistungsnachweise müssen in einem nachvollziehbaren und funktionalen Verhältnis zueinander stehen. Diese Abstimmung ist eine Voraussetzung dafür, dass das Curriculum weder inhaltlich überfrachtet noch methodisch widersprüchlich gestaltet wird und dass seine Wirkungsansprüche klar benannt und überprüfbar gemacht werden können. Ein Curriculum ist dann kohärent, wenn die einzelnen Bestandteile nicht additiv nebeneinanderstehen, sondern aufeinander aufbauen und gemeinsam zur Entwicklung der angestrebten Kompetenzen beitragen.

Fehlt eine solche Kohärenz, besteht die Gefahr, dass Inhalte zwar fachlich korrekt, didaktisch jedoch unverbunden bleiben oder dass Prüfungen andere Leistungen messen als jene, die in Modulen tatsächlich aufgebaut werden sollen. Für die Qualitätssicherung bedeutet dies, dass nicht allein einzelne Ausbildungsbestandteile bewertet werden dürfen, sondern immer auch ihr Zusammenhang innerhalb der Gesamtarchitektur in den Blick zu nehmen ist.

Ein drittes Grundprinzip ist das Prinzip der Mehrdimensionalität der Evaluation. Die Beurteilung von Ausbildungsqualität darf nicht auf eine einzige Ebene reduziert werden, etwa auf Zufriedenheit, Prüfungsergebnisse oder Teilnahmequoten. Vielmehr ist zwischen mehreren Wirkungsebenen zu unterscheiden. Eine erste Ebene betrifft die Reaktion der Teilnehmenden auf das Ausbildungsformat, beispielsweise hinsichtlich Verständlichkeit, Relevanz oder methodischer Plausibilität. Eine zweite Ebene betrifft den tatsächlichen Wissens- und Kompetenzzuwachs, also die Frage, ob Teilnehmende nach Abschluss eines Ausbildungsabschnitts über vertiefte Kenntnisse, verbesserte Analysefähigkeiten und höhere Handlungssicherheit verfügen. Eine dritte Ebene betrifft den Transfer in das berufliche Handeln, also ob das Gelernte im Dienstbetrieb, in Übungen, im Schichtdienst oder in Lagesituationen tatsächlich angewendet werden kann. Eine vierte Ebene betrifft schließlich die organisationale Wirkung, etwa im Sinne verbesserter Zusammenarbeit, klarerer Eskalationswege, beschleunigter Reaktionsketten, höherer Lagequalität oder robusterer betrieblicher Resilienz [141]. Gerade diese mehrdimensionale Sicht ist für militärische Ausbildung zentral, weil positive Rückmeldungen zu einem Lehrgang noch keinen belastbaren Fähigkeitszuwachs belegen und individueller Kompetenzaufbau nicht automatisch zu organisationaler Wirksamkeit führt.

Ein viertes Grundprinzip ist das Prinzip der Verbindung quantitativer und qualitativer Indikatoren. Ein belastbares Qualitätssystem muss unterschiedliche Formen der Evidenz miteinander verknüpfen. Quantitative Kennzahlen wie Teilnahme- und Erfolgsquoten, Prüfungsergebnisse, Wiederholungsbedarfe, Bearbeitungszeiten in Übungsszenarien oder Zeitwerte bei Erkennung, Bewertung und Eskalation von Vorfällen liefern wichtige Hinweise auf Struktur, Belastung und Leistung. Sie erlauben insbesondere dann belastbare Aussagen, wenn sie über mehrere Ausbildungsdurchgänge hinweg vergleichbar erhoben werden. Quantitative Daten allein reichen jedoch nicht aus, um Ausbildungsqualität in komplexen militärischen Cyber- und NOC-/SOC-Kontexten angemessen zu erfassen. Ebenso wichtig sind qualitative Beobachtungen, etwa zur Qualität von Lagebildern, zur Plausibilität technischer Hypothesen, zur Güte von Teamkommunikation, zur Angemessenheit von Eskalationen, zur Einhaltung rechtlicher und organisatorischer Vorgaben oder zum Fähigkeitserleben der Teilnehmenden beim Übergang in den Dienstbetrieb. Erst das Zusammenspiel dieser Perspektiven erlaubt eine belastbare Beurteilung, ob ein Modul fachlich tragfähig, didaktisch wirksam und operationell anschlussfähig ist.

Ein fünftes Grundprinzip ist das Prinzip der Transfer- und Wirkungsorientierung. Die Qualität eines Curriculums bemisst sich nicht allein daran, ob Inhalte erfolgreich vermittelt oder in Prüfungen reproduziert werden können, sondern daran, ob die aufgebauten Kompetenzen in realen Arbeits-, Führungs- und Einsatzkontexten wirksam werden. Für militärische Ausbildungsarchitekturen ist dies von besonderer Bedeutung, da Lernerfolg nicht in einem abstrakten Bildungsraum verbleiben darf, sondern sich im Dienstbetrieb, in Übungen und gegebenenfalls im Einsatz bewähren muss. Qualitätssicherung muss deshalb ausdrücklich den Übergang zwischen Ausbildung und Praxis in den Blick nehmen. Dies schließt die Frage ein, ob Absolventinnen und Absolventen in der Lage sind, sicherheitsrelevante Sachverhalte belastbar einzuordnen, in standardisierte Prozesse einzubringen, mit anderen Rollen zusammenzuarbeiten und unter Bedingungen von Unsicherheit, Zeitdruck und Arbeitsteilung professionell zu handeln. Ein Curriculum kann nur dann als wirksam gelten, wenn seine Ergebnisse nicht nur im Lehrgangsraum, sondern auch im operationellen Kontext beobachtbar werden.

Ein sechstes Grundprinzip ist das Prinzip der Evidenzbasierung. Anpassungen des Curriculums dürfen nicht allein auf subjektiven Eindrücken, kurzfristigen Trends oder vereinzelt Rückmeldungen beruhen. Vielmehr müssen sie auf systematisch erhobenen Beobachtungen, Evaluationsergebnissen, Prüfungsleistungen, Übungserfahrungen, Rückmeldungen aus dem Dienstbetrieb sowie auf Erkenntnissen aus technologischen und regulatorischen Entwicklungen aufbauen. Evidenzbasierung bedeutet dabei nicht, dass ausschließlich messbare Größen relevant sind. Auch qualitative Rückmeldungen, Erfahrungswissen aus Übungen oder strukturierte Debriefings können wertvolle Evidenz darstellen, sofern sie methodisch nachvollziehbar erhoben, dokumentiert und ausgewertet werden. Für die Qualitätssicherung ist dies deshalb bedeutsam, weil nur auf dieser Grundlage entschieden werden kann, ob festgestellte Defizite auf inhaltliche Lücken, methodische Schwächen, unklare Rollenlogiken oder unzureichende Transfermöglichkeiten zurückzuführen sind. Evidenzbasierung schützt das Curriculum damit vor willkürlicher Veränderung und stärkt zugleich seine Anschlussfähigkeit an reale Erfahrungs- und Entwicklungsprozesse.

Ein siebtes Grundprinzip ist das Prinzip der kontinuierlichen Weiterentwicklung. In einem technologisch dynamischen und sicherheitspolitisch volatilen Feld wie dem militärischen Cyber- und Informationsraum kann Curriculumsqualität nicht als statischer Zustand verstanden werden. Neue Bedrohungsformen, sich wandelnde technische Architekturen, veränderte regulatorische Anforderungen, neue Formen der Interoperabilität und gewonnene Erfahrungen aus Übungen und Einsätzen erfordern eine fortlaufende Überprüfung und Anpassung der Ausbildungsarchitektur. Weiterentwicklung bedeutet dabei jedoch nicht bloß Erweiterung. Ein professionell gepflegtes Curriculum muss ebenso in der Lage sein, Überfrachtungen zu reduzieren, Redundanzen zu identifizieren, veraltete Inhalte zu entfernen und Prioritäten neu zu gewichten. Kontinuierliche Weiterentwicklung ist daher nicht Ausdruck mangelnder Stabilität, sondern ein Merkmal curricularer Reife. Sie sorgt dafür, dass der curriculare Kern verlässlich bleibt, während spezifische Inhalte, Methoden und Szenarien an veränderte Rahmenbedingungen angepasst werden können.

Ein achttes Grundprinzip ist das Prinzip der institutionellen Verankerung. Qualitätssicherung darf nicht vom Zufall einzelner Erfahrungsberichte oder vom Engagement einzelner Lehrender abhängen. Sie benötigt geregelte Prozesse, definierte Verantwortlichkeiten und institutionelle Rückkopplungsschleifen, damit Erkenntnisse aus Evaluation, Übung, Prüfung und Praxis systematisch in die Weiterentwicklung des Curriculums einfließen können. Gerade im militärischen Kontext ist dies von besonderer Bedeutung, da personelle Rotation, unterschiedliche Vorverwendungen, organisationsspezifische Besonderheiten und wechselnde Einsatzanforderungen eine hohe institutionelle Stabilität der Ausbildungslogik erfordern. Eine institutionell verankerte Qualitätssicherung schafft Verlässlichkeit, Vergleichbarkeit und Nachvollziehbarkeit. Sie stellt sicher, dass Qualitätsentwicklung nicht episodisch oder personenbezogen erfolgt, sondern als dauerhafte Aufgabe des Gesamtsystems verstanden wird.

Schließlich folgt die Qualitätssicherung dem Prinzip der Balance zwischen Stabilität und Anpassungsfähigkeit. Ein Curriculum muss einen belastbaren Kern aus unverzichtbaren Kompetenzen, Begriffen und Handlungslogiken bewahren, um Vergleichbarkeit, Professionalität und Orientierung zu sichern. Zugleich muss es offen genug bleiben, um auf veränderte technische, operative und organisatorische Bedingungen reagieren zu können. Ein zu starres Curriculum verliert in dynamischen Feldern rasch an Relevanz; ein zu flexibles Curriculum riskiert hingegen den Verlust innerer Kohärenz und Verbindlichkeit. Qualitätssicherung hat daher auch die Aufgabe, diese Balance aktiv zu gestalten. Sie schützt den stabilen Kern der Ausbildung und ermöglicht zugleich gezielte, nachvollziehbare und begründete Anpassung.

5.9.2 Evaluations- und Reviewmechanismen

Evaluations- und Reviewmechanismen sind als zentrale Steuerungsinstrumente eines kompetenzorientierten Curriculums zu verstehen. Sie dienen nicht allein der nachträglichen Bewertung einzelner Ausbildungsmaßnahmen, sondern der fortlaufenden Überprüfung, ob Ziele, Inhalte, Methoden und Leistungsnachweise tatsächlich geeignet sind, die angestrebten Kompetenzen aufzubauen und unter realen Bedingungen wirksam werden zu lassen. Für ein militärisches Curriculum im Cyber- und Informationsraum ist dies von besonderer Bedeutung, weil sich Ausbildungsqualität nicht ausschließlich an der formalen Durchführung von Modulen oder an punktuellen Prüfungsergebnissen bemisst. Entscheidend ist vielmehr, ob Ausbildung im gesamten Zyklus – von der Ausgangslage der Teilnehmenden über den Lernprozess bis hin zur späteren Verwendung – so gestaltet und überprüft wird, dass fachliche Belastbarkeit, methodische Wirksamkeit und operationelle Anschlussfähigkeit systematisch gesichert werden können. Evaluation und Review sind daher nicht als ergänzende Zusatzfunktionen zu begreifen, sondern als integrale Bestandteile curricularer Steuerung und Weiterentwicklung.

Auf der Ebene der Durchführung sollten Evaluations- und Reviewmechanismen entlang des gesamten Ausbildungszyklus verankert werden. Bereits vor Beginn eines Moduls können Eingangserhebungen genutzt werden, um Vorkenntnisse, Erwartungshaltungen, berufliche Vorerfahrungen und typische Kompetenzlücken sichtbar zu machen. Solche Erhebungen besitzen nicht nur diagnostischen Wert, sondern erfüllen auch eine didaktische Steuerungsfunktion. Sie ermöglichen es, Module besser auf die tatsächliche Ausgangslage der Teilnehmenden abzustimmen, Schwerpunkte bewusster zu setzen und potenzielle Fehlanpassungen zwischen Anspruchsniveau und Vorkenntnissen frühzeitig zu erkennen. Gerade in militärischen Ausbildungszusammenhängen, in denen Teilnehmende häufig aus unterschiedlichen Verwendungen, Organisationsbereichen und Erfahrungsräumen kommen, ist diese Eingangsperspektive besonders relevant. Ohne eine systematische Erfassung der Ausgangslage besteht die Gefahr, dass Ausbildung entweder unterfordernd bleibt oder an den tatsächlichen Lernvoraussetzungen vorbeigeht. Während des Moduls gewinnen formative Evaluationsverfahren besondere Bedeutung. Darunter sind Verfahren zu verstehen, die den Lernprozess fortlaufend begleiten und Hinweise darauf liefern, ob Lernfortschritt, didaktische Passung und methodische Angemessenheit tatsächlich gegeben sind. Hierzu zählen etwa kurze Wissenschecks, Beobachtungen in Übungen, Debriefings, Peer-Feedback, strukturierte Reflexionsaufgaben oder moderierte Zwischenrückmeldungen. Der Wert solcher Verfahren liegt darin, dass sie nicht erst am Ende bilanzieren, ob Lernerfolg eingetreten ist, sondern bereits im Verlauf sichtbar machen, wo Verständnisprobleme, Fehlannahmen, Überforderungen oder didaktische Schwächen bestehen. Dies ist für ein Curriculum im militärischen Cyber- und Informationsraum besonders wichtig, weil sich dort viele Kompetenzerfordernisse erst im Handeln unter Unsicherheit, Zeitdruck und Kooperationsbedarf zeigen. Formative Verfahren erlauben es, dieses Handeln frühzeitig zu beobachten und gezielt nachzusteuern. Sie schaffen damit die Voraussetzung für ein lernendes Ausbildungssystem, das nicht erst Defizite feststellt, wenn ein Modul bereits abgeschlossen ist, sondern während der Durchführung auf erkannte Probleme reagieren kann.

Nach Abschluss eines Moduls sind summative Verfahren erforderlich, um Lernerfolg, Transferpotenzial und Verbesserungsbedarfe systematisch zu dokumentieren. Summative Evaluation dient der Bilanzierung dessen, was am Ende eines Ausbildungsabschnitts tatsächlich erreicht wurde. Dazu gehören klassisch Prüfungsleistungen, beobachtete Kompetenzdemonstrationen in Szenarien, dokumentierte Übungsergebnisse oder strukturierte Abschlussbefragungen. Im vorliegenden Kontext ist jedoch entscheidend, dass summative Verfahren nicht auf die reine Wissensreproduktion beschränkt bleiben. Vielmehr sollten sie darauf abzielen, zu erfassen, inwieweit Teilnehmende in der Lage sind, Fachwissen in Lageverstehen, Priorisierung, Kommunikation und koordiniertes Handeln zu überführen. Gerade in militärischen

SOC- und NOC-Kontexten wäre eine summative Bewertung unzureichend, wenn sie ausschließlich auf die korrekte Wiedergabe technischer Begriffe oder Verfahrensschritte abstellt. Erforderlich ist vielmehr eine Bewertung, die auch die Fähigkeit erfasst, in realitätsnahen Situationen mit Unsicherheit, Zeitdruck und arbeitsteiliger Koordination umzugehen. Die Kombination aus diagnostischen, formativen und summativen Verfahren verhindert daher, dass Qualitätssicherung erst am Ende eines Ausbildungszyklus ansetzt und lediglich feststellt, wo Defizite bestanden, ohne rechtzeitig gegensteuern zu können. Für ein militärisches Curriculum ist besonders bedeutsam, dass Evaluation nicht nur aus Sicht der Teilnehmenden, sondern auch aus Sicht der späteren Verwendung erfolgt. Ausbildung kann nur dann als wirksam gelten, wenn ihre Ergebnisse sich nicht allein im Lehrgangsraum, sondern auch im Arbeits- und Einsatzkontext bewähren. Rückmeldungen aus dem Schichtbetrieb, aus Übungen, aus Stäben und aus Vorgesetztenbeurteilungen liefern daher unverzichtbare Hinweise darauf, ob Ausbildungsinhalte im realen Arbeitskontext tragfähig sind. Solche Rückmeldungen machen sichtbar, ob Absolventinnen und Absolventen tatsächlich in der Lage sind, standardisierte Prozesse anzuwenden, Schnittstellen professionell zu bedienen, sicherheitsrelevante Sachverhalte angemessen zu bewerten und in organisationsbezogene Handlungslogiken einzubringen. Hierzu können strukturierte Nachbefragungen nach einigen Monaten, Beobachtungen in Folgeübungen, Rückmeldungen aus dem Einsatz- oder Schichtkontext sowie die Analyse typischer Fehler- und Unterstützungsbedarfe herangezogen werden. Die arbeitsplatzbezogene Perspektive ist besonders wichtig, weil Ausbildungswirksamkeit im militärischen Bereich nicht allein in individuellem Lernerfolg besteht, sondern in der Frage, ob sich dieser Lernerfolg in belastbare professionelle Leistung und organisationale Einsatzfähigkeit übersetzt.

Moderne Cyber-Workforce-Ansätze betonen in diesem Zusammenhang, dass Kompetenzentwicklung nur dann wirksam steuerbar ist, wenn Ausbildungsleistungen mit arbeitsplatznahen Aufgabenprofilen und Proficienzniveaus rückgekoppelt werden [138], [140]. Das bedeutet, dass Evaluation nicht nur schulisch oder kursbezogen erfolgen darf, sondern ausdrücklich arbeitsplatzbezogen ausgerichtet sein muss. Die Frage lautet dann nicht mehr nur, ob ein Modul didaktisch gelungen war oder ob Teilnehmende ein Thema verstanden haben, sondern ob die vermittelten Kompetenzen in den tatsächlichen Rollenprofilen, Verantwortungsbereichen und Belastungssituationen späterer Verwendungen tragfähig sind. Damit wird Evaluation zu einem Bindeglied zwischen Curriculum, Personalentwicklung und Fähigkeitsmanagement. Sie trägt dazu bei, Ausbildungsinhalte nicht isoliert zu betrachten, sondern in Relation zu realen Aufgaben, Kompetenzstufen und organisationsbezogenen Anforderungen zu bewerten. Reviewmechanismen betreffen darüber hinaus nicht nur Lernergebnisse, sondern auch Inhalte, Szenarien und curriculare Annahmen. Da sich Bedrohungen, Technologien, Führungsanforderungen und Organisationsstrukturen im militärischen Cyber- und Informationsraum fortlaufend verändern, müssen Module in festgelegten Intervallen überprüft werden. Ein jährlicher oder anlassbezogener Review-Zyklus – etwa nach größeren Übungen, realen Vorfällen, technischen Umstellungen oder relevanten Strukturänderungen – ermöglicht es, Inhalte gezielt zu aktualisieren und curriculare Relevanz zu erhalten. Dies umfasst beispielsweise die Ersetzung veralteter Fallstudien, die Integration neuer Angriffs- oder Störungsmuster, die Anpassung von Schnittstellenbeschreibungen, die Aktualisierung von Lehrmaterialien oder die Überarbeitung von Übungsarchitekturen. Ein solcher Review-Prozess ist nicht Ausdruck mangelnder curricularer Stabilität, sondern gerade Voraussetzung dafür, dass ein Curriculum in einem dynamischen Umfeld langfristig belastbar bleibt. Dabei ist wesentlich, dass Reviews nicht beliebig oder rein reaktiv erfolgen, sondern entlang klar definierter Kriterien und Prozesse strukturiert sind. Zu prüfen ist etwa, ob bestehende Lernziele weiterhin den relevanten Kompetenzbedarf abbilden, ob die in Modulen eingesetzten Szenarien noch repräsentativ für aktuelle Bedrohungs- und Betriebsrealitäten sind, ob Prüfungsformate tatsächlich die angestrebten Kompetenzen erfassen und ob neue technologische oder organisatorische Entwicklungen Anpassungen erforderlich machen. Ebenso wichtig ist die Frage, ob Inhalte möglicherweise

überholt, redundant oder überfrachtend geworden sind. Ein professioneller Review-Mechanismus dient daher nicht nur der Erweiterung des Curriculums, sondern ebenso seiner Fokussierung und Priorisierung. Gerade in technologisch dynamischen Feldern besteht sonst die Gefahr, dass neue Themen fortlaufend ergänzt werden, ohne veraltete oder weniger relevante Bestandteile systematisch zurückzunehmen. Frameworks wie NICE und ECSF zeigen, dass curriculare Stabilität und flexible Aktualisierung kein Widerspruch sind, sondern durch eine klare Trennung von stabilem Kompetenzkern und adaptiver Umsetzungsschicht organisiert werden können [138], [139]. Diese Unterscheidung ist auch für das vorliegende Curriculum besonders tragfähig. Der stabile Kern umfasst jene grundlegenden Kompetenzen, Begriffe, Handlungslogiken und professionellen Anforderungen, die unabhängig von konkreten Technologien oder aktuellen Bedrohungsausprägungen dauerhaft relevant bleiben. Die adaptive Umsetzungsschicht betrifft demgegenüber jene Elemente, die in kürzeren Zyklen angepasst werden müssen, etwa konkrete Fallstudien, Werkzeuge, Szenarien, Angriffsformen, Kommunikationsschnittstellen oder Übungsparameter. Ein systematischer Review-Mechanismus muss beide Ebenen auseinanderhalten: Er muss einerseits den Kern des Curriculums schützen, um Kohärenz, Vergleichbarkeit und Professionalität zu sichern, und andererseits die Umsetzungsschicht aktiv an veränderte Rahmenbedingungen anpassen.

5.9.3 Weiterentwicklung, Governance und Lessons Learned

Die Weiterentwicklung des Curriculums ist nicht als gelegentliche Überarbeitung einzelner Inhalte, sondern als dauerhafte Governance-Aufgabe zu verstehen. In einem technologisch dynamischen und sicherheitskritischen Feld wie dem militärischen Cyber- und Informationsraum kann curriculare Qualität nur dann langfristig gesichert werden, wenn Verfahren der Evaluation, Priorisierung und Anpassung institutionell verankert sind. Weiterentwicklung darf daher weder dem Zufall informeller Rückmeldungen noch der punktuellen Reaktion auf Einzelereignisse überlassen werden. Vielmehr bedarf es klarer Zuständigkeiten dafür, wer Evaluationsergebnisse sammelt, auswertet, priorisiert und in curricular wirksame Entscheidungen übersetzt. Governance meint in diesem Zusammenhang die geregelte organisatorische Verantwortungsstruktur, durch die sichergestellt wird, dass Qualitätssicherung, Review und Anpassung nicht nur fachlich begründet, sondern auch transparent, nachvollziehbar und nachhaltig umgesetzt werden.

Ein belastbares Governance-Modell setzt voraus, dass Weiterentwicklung nicht allein aus der Perspektive der Ausbildung gedacht wird. Ein Curriculum im militärischen Cyber- und Informationsraum steht an der Schnittstelle von Fachlichkeit, Betrieb, Führung, Recht, Übungswesen und organisatorischer Realisierbarkeit. Deshalb ist es sinnvoll, die Weiterentwicklung in einem regelmäßigen Review-Gremium zu verankern, in dem unterschiedliche Perspektiven zusammengeführt werden. Ein solches Gremium sollte aus fachlicher Leitung, Ausbildungspersonal, Vertreterinnen und Vertretern des Betriebs, gegebenenfalls aus der Rechtsberatung sowie – wo relevant – aus OT-, Übungs- oder Stabsbereichen zusammengesetzt sein. Die Stärke eines solchen Gremiums liegt gerade in seiner Mehrperspektivität. Veränderungen können dadurch nicht nur fachlich-inhaltlich, sondern auch im Hinblick auf Realisierbarkeit, Geheimschutz, Ressourcenbedarf, Interoperabilität und organisationspraktische Folgen eingeordnet werden. Dies ist für militärische Ausbildungsarchitekturen besonders bedeutsam, weil curriculare Entscheidungen regelmäßig nicht nur didaktische, sondern auch sicherheitsbezogene, technische und institutionelle Implikationen besitzen.

Die institutionelle Verankerung eines solchen Review-Mechanismus verhindert, dass Curricula entweder zufällig fortgeschrieben oder ausschließlich reaktiv an Einzelereignisse angepasst werden. Ohne geregelte Governance besteht die Gefahr, dass Weiterentwicklung von Einzelinteressen, kurzfristigen Eindrücken oder punktuellen Problemwahrnehmungen dominiert wird. Ein strukturiertes Gremium schafft demgegenüber die Voraussetzung für Priorisierung und

Abwägung. Nicht jede neue Beobachtung, jede technologische Entwicklung oder jede Übungserfahrung muss unmittelbar zu curricularen Veränderungen führen. Entscheidend ist vielmehr, welche Beobachtungen wiederkehrend, sicherheitsrelevant, rollenübergreifend oder strategisch bedeutsam sind. Governance bedeutet daher auch, zwischen episodischen Einzelbefunden und strukturell relevanten Entwicklungssignalen unterscheiden zu können. Erst diese Form der institutionellen Filterung macht aus einer Vielzahl von Rückmeldungen eine belastbare Grundlage für curricular wirksame Entscheidungen.

In diesem Zusammenhang kommt Lessons Learned eine zentrale Funktion zu. Sie sollten nicht als lose Sammlung von Erfahrungen verstanden werden, sondern als strukturierter Datenstrom, der systematisch in die Weiterentwicklung des Curriculums eingespeist wird. Relevante Quellen hierfür sind Debriefings aus Cyber-Range-Übungen, Abschlussprüfungen, Realvorfälle, Audits, technische Nachanalysen, Beobachtungen aus dem Schichtbetrieb sowie Rückmeldungen aus Führungs- und Einsatzkontexten. Diese Quellen unterscheiden sich hinsichtlich ihres Detaillierungsgrads, ihrer Perspektive und ihrer Aussagekraft, liefern jedoch zusammengekommen ein vielschichtiges Bild darüber, wo ein Curriculum tragfähig ist und wo Anpassungsbedarf besteht. Debriefings aus Cyber-Range-Szenarien können etwa auf Schwächen in Lagekommunikation, Schnittstellenarbeit oder Priorisierung hinweisen. Realvorfälle und technische Nachanalysen machen sichtbar, ob bestimmte Bedrohungsformen, Abhängigkeiten oder Betriebslogiken im Curriculum bislang unzureichend adressiert werden. Beobachtungen aus Schichtbetrieb und Vorgesetztenrückmeldungen liefern Hinweise darauf, ob Ausbildungsinhalte im realen Arbeitskontext tatsächlich anschlussfähig und handlungswirksam sind. Entscheidend ist jedoch, dass solche Erfahrungen nicht nur gesammelt, sondern in curricular verwertbare Kategorien übersetzt werden. Erst diese Übersetzungsleistung macht Lessons Learned für die Weiterentwicklung produktiv. Zu fragen ist etwa: Welche Wissensgebiete sind systematisch unterrepräsentiert? Wo fehlen methodische Routinen? Welche Playbooks, Eskalationslogiken oder Kommunikationsmuster erweisen sich in Übungen oder Realfällen als unklar? Welche Schnittstellen werden wiederholt problematisch? Wo zeigen sich Defizite im Übergang zwischen Analyse, Betrieb und Führung? Welche Kompetenzanforderungen wurden im Curriculum bislang zu niedrig oder zu hoch angesetzt? Solche Fragen transformieren beobachtete Einzelereignisse in strukturierte Lernsignale für das Curriculum. Ohne diese analytische Verdichtung blieben Lessons Learned auf der Ebene bloßer Ereignissammlung stehen und würden keinen systematischen Beitrag zum organisationalen Lernen leisten. Damit aus Erfahrung tatsächlich organisationales Lernen entsteht, müssen Beobachtungen standardisiert dokumentiert, verglichen und priorisiert werden. Es reicht nicht aus, nach Übungen oder Vorfällen isolierte Erfahrungsberichte zu erstellen, wenn diese nicht in eine gemeinsame Auswertungslogik eingebettet sind. Ein professioneller Lessons-Learned-Prozess benötigt daher Kriterien, nach denen Befunde geordnet und bewertet werden können. Dazu gehört beispielsweise die Unterscheidung zwischen fachlichen Inhaltslücken, methodischen Defiziten, unklaren Rollenprofilen, unzureichend trainierten Kommunikationsmustern oder strukturellen Problemen an Schnittstellen. Ebenso relevant ist die Frage nach Häufigkeit, Tragweite und Wiederholungswahrscheinlichkeit eines Problems. Erst wenn Erfahrungen auf diese Weise systematisch verdichtet werden, entsteht eine Wissensbasis, auf deren Grundlage das Curriculum nicht nur punktuell korrigiert, sondern gezielt weiterentwickelt werden kann.

Die Weiterentwicklung des Curriculums ist somit als ein geregelter Prozess zu verstehen, in dem Evaluation, Governance und Lessons Learned ineinandergreifen. Evaluation liefert Daten und Beobachtungen, Governance schafft die institutionellen Entscheidungsstrukturen, und Lessons Learned sorgen dafür, dass Erfahrungen aus Ausbildung, Betrieb und Einsatz in verwertbarer Form in das Curriculum zurückfließen. Diese Rückkopplung ist für die langfristige Wirksamkeit des Curriculums von zentraler Bedeutung. Gerade im militärischen Cyber- und Informationsraum, der durch hohe Innovationsgeschwindigkeit, dynamische Bedrohungslagen und steigende



Anforderungen an Interoperabilität geprägt ist, genügt es nicht, ein Curriculum einmal fachlich korrekt zu entwerfen. Es muss vielmehr dauerhaft überprüfbar, anpassungsfähig und zukunftsfähig bleiben. Qualitätssicherung und Weiterentwicklung tragen damit wesentlich zur strategischen Belastbarkeit des Curriculums bei. Strategische Belastbarkeit bedeutet in diesem Zusammenhang, dass das Curriculum nicht nur kurzfristig funktional ist, sondern auch unter veränderten technischen, organisatorischen und sicherheitspolitischen Bedingungen seine Relevanz und Wirksamkeit bewahren kann. Ein Curriculum, das kontinuierlich überprüft, reflektiert und angepasst wird, ist besser in der Lage, neue Anforderungen aufzunehmen, veraltete Inhalte zu identifizieren und seine Ausbildungslogik an veränderte operative Realitäten anzupassen. Es wird dadurch selbst zu einem Bestandteil organisationaler Resilienz. Für ein militärisches Ausbildungsprogramm im Cyber- und Informationsraum bedeutet dies, dass Qualität nicht als Ergebnis einmaliger Perfektion verstanden werden darf. Sie ist vielmehr das Resultat eines disziplinierten, evidenzbasierten und verantworteten Verbesserungsprozesses. Gerade in einem Umfeld, in dem technologische Veränderung und operationeller Druck gleichzeitig zunehmen, wird ein solcher Prozess selbst zu einer sicherheitsrelevanten Fähigkeit der Organisation.

6 Durchgeführte Trainings

Mit dem entwickelten Curriculum, der konzipierten Trainingsumgebung sowie den darauf aufbauenden Trainingsunterlagen liegt im Projekt Bumblebee ein konsistenter Ausbildungsrahmen für den militärischen Cyberkontext vor. Die Belastbarkeit eines solchen Rahmens kann jedoch nicht allein aus der konzeptionellen Herleitung abgeleitet werden, sondern muss unter realitätsnahen Anwendungsbedingungen empirisch geprüft werden. Vor diesem Hintergrund dokumentiert das vorliegende Kapitel die im Projektverlauf durchgeführten Trainings als zentrale Phase der praktischen Erprobung, Validierung und schrittweisen Weiterentwicklung der entwickelten Ausbildungsansätze.

Im Mittelpunkt steht dabei die Frage, inwiefern die konzipierten Inhalte, didaktischen Formate und technischen Umgebungen geeignet sind, die in den vorangegangenen Kapiteln beschriebenen Kompetenzziele in einer realen Trainingssituation zu unterstützen. Die durchgeführten Übungen sind daher nicht lediglich als isolierte Einzelveranstaltungen zu verstehen, sondern als aufeinander bezogene Erprobungsräume, in denen curriculare Annahmen, methodische Entscheidungen und infrastrukturelle Voraussetzungen systematisch überprüft und iterativ weiterentwickelt wurden. Das Kapitel rekonstruiert diese Entwicklung entlang der vier im Projektzeitraum durchgeführten Cyber-Übungen und zeigt, wie sich aus den jeweiligen Evaluierungsergebnissen konkrete Implikationen für die Weiterentwicklung des Ausbildungsprogramms ableiten ließen.

6.1 Einordnung des Evaluationsabschnitts und Projekthintergrund

Das Projekt Bumblebee verfolgt das Ziel, das Bundesministerium für Landesverteidigung beim Aufbau einer eigenständigen, strukturierten und nachhaltig anschlussfähigen Ausbildung zukünftiger Cyber-Kräfte zu unterstützen. Ausgangspunkt hierfür war eine systematische Bedarfs- und Anforderungsanalyse, auf deren Grundlage sowohl ein Curriculum für die Ausbildung im Cybersecurity-Bereich als auch ein Konzept für eine flexible und praxisnahe Trainingsplattform entwickelt wurden. Aufbauend auf diesen konzeptionellen Grundlagen wurden in einem weiteren Schritt konkrete Ausbildungsunterlagen für Auszubildende sowie Formate für Train-the-Trainer-Szenarien erarbeitet.

Das Arbeitspaket 5 „Demonstration und Evaluierung“ übernimmt innerhalb dieser Gesamtlogik eine zentrale Funktion. Während die vorangegangenen Arbeitspakete auf die konzeptionelle Herleitung, curriculare Strukturierung und didaktisch-technische Ausgestaltung des Ausbildungsansatzes fokussieren, dient Arbeitspaket 5 der empirischen Überprüfung seiner praktischen Tragfähigkeit. Ziel ist es, die entwickelten Curricula, Trainingsformate, Übungsunterlagen und infrastrukturellen Elemente unter realitätsnahen Bedingungen zu erproben und ihre Eignung im Hinblick auf Relevanz, Umsetzbarkeit und Lernwirksamkeit zu bewerten. Die Ergebnisse dieser Erprobungen fließen wiederum in die Weiterentwicklung der konzeptionellen und didaktischen Bausteine des Projekts zurück und sichern damit einen evidenzbasierten, iterativen Verbesserungsprozess. Die im Antrag definierten Meilensteine des Arbeitspakets 5 bilden diesen Entwicklungsprozess in strukturierter Form ab. Mit M 5.1 wurde zunächst ein Evaluierungskonzept erstellt, das die einheitliche und nachvollziehbare Bewertung aller relevanten Projektkomponenten ermöglichen sollte. Darauf aufbauend war mit M 5.2 die Durchführung und Auswertung einer ersten Cyber-Übung vorgesehen, um frühe Hinweise auf die Tragfähigkeit der Ausbildungsinhalte und mögliche Verbesserungsbedarfe zu gewinnen. M 5.3 sah schließlich die Durchführung und Auswertung weiterer Übungen zur vertieften Validierung der weiterentwickelten Konzepte vor.

Im tatsächlichen Projektverlauf wurden insgesamt vier Cyber-Übungen durchgeführt und damit zwei mehr als ursprünglich vorgesehen. Diese Erweiterung erfolgte in Abstimmung mit dem

Bedarfsträger und erwies sich aus analytischer Sicht als besonders wertvoll. Die zusätzliche Erprobung ermöglichte eine breitere empirische Grundlage, eine schrittweise Verdichtung der Evaluierungsergebnisse sowie eine differenziertere Rückkopplung zwischen curricularer Entwicklung, didaktischer Gestaltung und technischer Trainingsumgebung. Die durchgeführten Trainings sind daher als integraler Bestandteil des Gesamtprojekts zu verstehen: Sie dienten nicht nur der abschließenden Bewertung, sondern fungierten zugleich als zentrale Lern- und Anpassungsschleife innerhalb des Entwicklungsprozesses.

6.2 Evaluationsdesign und methodisches Vorgehen

Zur Einordnung der nachfolgend dargestellten Trainings und ihrer Ergebnisse ist zunächst das zugrunde liegende Evaluationsdesign zu erläutern. Die im Projekt Bumblebee durchgeführten Übungen dienten nicht allein der Durchführung einzelner Ausbildungsmaßnahmen, sondern waren zugleich als systematische Erprobungs- und Validierungsschritte angelegt. Entsprechend war es erforderlich, ein methodisches Vorgehen zu definieren, das sowohl die Bewertung der inhaltlichen und didaktischen Qualität als auch die Einschätzung der technischen und organisatorischen Rahmenbedingungen ermöglicht. Die folgenden Unterabschnitte beschreiben daher die Zielsetzungen der Evaluierung, den methodischen Ansatz, die zugrunde gelegten Evaluationsdimensionen sowie die konkrete Durchführung der Datenerhebung und Auswertung.

6.2.1 Evaluationsziele

Das im Projekt angewandte Evaluationskonzept verfolgte mehrere miteinander verknüpfte Zielsetzungen. Im Zentrum stand zunächst die Validierung der entwickelten Ausbildungsinhalte. Geprüft werden sollte, ob die erarbeiteten Module den Anforderungen der Zielgruppe entsprechen, inhaltlich als relevant wahrgenommen werden und einen nachvollziehbaren Beitrag zur Erreichung der definierten Lernziele leisten. Eng damit verbunden war die Frage nach der didaktischen Eignung der gewählten Formate, insbesondere hinsichtlich ihrer Wirksamkeit, Akzeptanz und Passung zur Heterogenität der Teilnehmenden.

Darüber hinaus bezog die Evaluierung ausdrücklich auch die technische Infrastruktur der Trainingsumgebung ein. Von Interesse war hierbei, inwiefern die eingesetzten Plattformen, Tools und Simulationsumgebungen stabil, benutzbar und für die Durchführung praxisnaher Trainingsszenarien geeignet sind. Die Evaluierung zielte somit nicht ausschließlich auf die Qualität einzelner Lehrinhalte, sondern auf das Zusammenwirken von Curriculum, didaktischer Umsetzung und technischer Umgebung.

Übergreifend diente das Evaluationskonzept der Etablierung einer kontinuierlichen Feedbackschleife. Die einzelnen Übungen sollten nicht isoliert bewertet werden, sondern als aufeinander aufbauende Erprobungsphasen fungieren, aus denen fortlaufend Hinweise für die Optimierung der Ausbildungsarchitektur gewonnen werden konnten. Die Evaluierung ist damit als konstitutiver Bestandteil einer evidenzbasierten Curriculumsentwicklung zu verstehen.

6.2.2 Methodischer Ansatz

Methodisch folgte die Evaluierung einem Mixed-Methods-Ansatz, in dem quantitative und qualitative Erhebungsinstrumente miteinander kombiniert wurden. Diese methodische Anlage war insofern zweckmäßig, als die Bewertung der Trainings nicht allein auf numerische Zufriedenheits- oder Schwierigkeitswerte reduziert werden sollte, sondern auch die subjektiven Wahrnehmungen, Begründungen und kontextbezogenen Erfahrungen der Teilnehmenden sowie die Beobachtungen des Trainerteams berücksichtigt werden mussten.

Die quantitative Dimension umfasste insbesondere standardisierte Online-Fragebögen zur Erfassung von Bewertungen, Selbsteinschätzungen und Zufriedenheit, strukturierte Skalen zur Einschätzung von Schwierigkeitsgrad, Lernzuwachs und Praxisrelevanz sowie vergleichende Erhebungen über mehrere Übungen hinweg. Dadurch konnten Entwicklungstendenzen sichtbar gemacht und Veränderungen im didaktischen Design oder im Verhältnis von Theorie und Praxis nachvollzogen werden.

Die qualitative Dimension ergänzte diese Befunde durch offene Freitextfelder, moderierte Feedbackrunden am Ende einzelner Trainingstage, Beobachtungsprotokolle des Trainerteams sowie informelle Gespräche während Pausen und Übungsphasen. Der Erkenntniswert dieser qualitativen Zugänge lag insbesondere darin, Hintergründe für Bewertungen sichtbar zu machen, Spannungen zwischen Erwartung und Erfahrung zu identifizieren und konkrete Hinweise für die Weiterentwicklung der Formate abzuleiten.

Die Auswertung folgte dem Prinzip der Triangulation. Quantitative und qualitative Daten wurden nicht getrennt voneinander betrachtet, sondern systematisch miteinander in Beziehung gesetzt, um ein möglichst differenziertes und belastbares Bild der Wirksamkeit der Trainingsformate zu gewinnen. Auf diese Weise konnte die Evaluierung sowohl aggregierte Tendenzen als auch kontextgebundene Einzelbeobachtungen berücksichtigen.

6.2.3 Evaluierungsdimensionen

Die Evaluierung orientierte sich an sieben zentralen Dimensionen, die gemeinsam eine mehrperspektivische Betrachtung der Trainings ermöglichen. Erfasst wurden erstens Merkmale der Zielgruppe, insbesondere Bildungsniveau, Vorerfahrungen und Motivation der Teilnehmenden. Zweitens wurde die inhaltliche Qualität der vermittelten Themenbereiche untersucht, etwa im Hinblick auf Relevanz, Aktualität und Verständlichkeit. Drittens standen Didaktik und Methodik im Fokus, insbesondere die Balance zwischen Theorie und Praxis, die Strukturierung der Übungseinheiten sowie die Anschlussfähigkeit der gewählten Formate an die Kompetenzniveaus der Zielgruppe.

Viertens wurde der Lernerfolg betrachtet, sowohl in Form subjektiver Selbsteinschätzungen als auch im Sinne der beobachtbaren Bewältigung von Aufgabenstellungen. Fünftens floss die technische Infrastruktur in die Bewertung ein, insbesondere hinsichtlich Stabilität, Performance und Benutzbarkeit der eingesetzten Trainingsumgebung. Sechstens wurden organisatorische Rahmenbedingungen wie Zeitmanagement, Räumlichkeiten und Verpflegung berücksichtigt. Siebtens bezog die Evaluierung auch die wahrgenommene Trainerkompetenz ein, darunter Fachkompetenz, didaktische Qualität und die Fähigkeit, konstruktives Feedback zu geben.

Diese Dimensionen bildeten zusammen einen analytischen Rahmen, der es ermöglichte, die Trainings nicht nur als isolierte Lehrveranstaltungen, sondern als komplexe Lernsituationen zu bewerten, in denen Inhalt, Methode, Infrastruktur und Organisation ineinandergreifen.

6.2.4 Durchführung der Evaluierung

Die Evaluierung war so angelegt, dass sie den gesamten Verlauf der jeweiligen Übung begleitete und Daten zu mehreren Zeitpunkten erhob. Bereits vor Beginn der Veranstaltungen wurden Vorkenntnisse, Erwartungen und Interessen der Teilnehmenden erfasst. Ergänzend dazu fanden Vorgespräche mit den Bedarfsträgern statt, um die institutionellen Zielsetzungen und den Erwartungshorizont für die Trainings zu präzisieren.

Während der Übungen selbst erfolgte eine kontinuierliche Beobachtung des Geschehens durch das Trainerteam. Ergänzend wurden informelle Gespräche in Pausen und Arbeitsphasen genutzt, um unmittelbare Eindrücke, Unsicherheiten und Rückmeldungen der Teilnehmenden aufzugreifen.



Am Ende einzelner Trainingstage wurden kurze moderierte Feedbackrunden durchgeführt, um erste Reaktionen in strukturierter Form zu erfassen. Nach Abschluss der Veranstaltungen erfolgte schließlich eine umfassendere Erhebung mittels Online-Fragebogen.

Die gewonnenen Erkenntnisse wurden im Anschluss projektintern ausgewertet, verdichtet und in Maßnahmen für die Weiterentwicklung des Curriculums, der Trainingsunterlagen und der Trainingsumgebung überführt. Damit war die Evaluierung nicht nur retrospektiv angelegt, sondern diente unmittelbar der formativen Optimierung der im Projekt entwickelten Ausbildungsarchitektur.

6.3 Übungen

Die im Projektverlauf durchgeführten Übungen bilden den operativen Kern der empirischen Erprobung und Validierung des entwickelten Ausbildungsansatzes. Sie dienen nicht allein der praktischen Durchführung einzelner Trainingsformate, sondern übernehmen zugleich eine analytische Funktion, indem sie sichtbar machen, inwieweit curriculare Annahmen, didaktische Konzepte und technische Rahmenbedingungen unter realitätsnahen Bedingungen tragfähig sind. Die Übungen sind damit als anwendungsorientierte Prüf- und Lernräume zu verstehen, in denen die im Projekt entwickelten Inhalte nicht nur vermittelt, sondern in ihrer praktischen Umsetzbarkeit, Anschlussfähigkeit und Wirksamkeit überprüft werden. Zugleich ermöglichen die Übungen eine schrittweise Verdichtung der im Projekt gewonnenen Erkenntnisse. Von frühen Erprobungsformaten über stärker strukturierte Trainings bis hin zur abschließenden mehrtägigen Validierungsübung wird nachvollziehbar, wie sich der Ausbildungsansatz iterativ weiterentwickelt hat. Das vorliegende Kapitel beschreibt die einzelnen Übungen daher nicht isoliert, sondern als zusammenhängende Entwicklungsschritte eines evidenzbasierten Qualifizierungsmodells, in dem fachliche Kompetenzentwicklung, didaktische Gestaltung und technische Trainingsumgebung in enger Wechselwirkung stehen.

6.3.1 Erste Cyber-Übung Februar 2024

Die erste Cyber-Übung bildete den Ausgangspunkt der praktischen Evaluierungsphase im Projekt Bumblebee. Ihr Charakter war in besonderem Maße explorativ, da sie nicht nur der ersten Erprobung eines Trainingsformats diente, sondern zugleich wesentliche Hinweise auf die Zusammensetzung, Vorkenntnisse und Erwartungen der Zielgruppe lieferte. Aus wissenschaftlicher Sicht ist diese Übung daher weniger als abschließende Validierung eines bereits ausgereiften Konzepts zu verstehen, sondern vielmehr als empirischer Ausgangspunkt für die nachfolgende curriculare und didaktische Weiterentwicklung. Die folgenden Unterabschnitte stellen zunächst das Übungskonzept und die Zielsetzung dar, fassen anschließend die zentralen Evaluierungsergebnisse zusammen und leiten daraus die wesentlichen Implikationen für die Weiterentwicklung des Ausbildungsprogramms ab.

6.3.1.1 Übungskonzept und Zielsetzung

Die erste Cyber-Übung fand am 08. Februar 2024 in der Landesverteidigungsakademie statt und markierte den Beginn der praktischen Evaluierungsphase des Projekts Bumblebee. Ziel der ganztägigen Veranstaltung war es, eine erste Bedarfserhebung mit der Zielgruppe zu verbinden und zugleich grundlegende Elemente des Ausbildungskonzepts sowie erste mögliche Übungsformate unter praxisnahen Bedingungen zu erproben. An der Übung nahmen 20 Personen teil.

Die Veranstaltung war als Kombination aus theoretischer Einführung und praktischer Übungsphase angelegt. Neben der Vermittlung grundlegender Konzepte stand insbesondere das Ziel im Vordergrund, erste Erfahrungen mit realitätsnahen Angriffsszenarien zu ermöglichen und ein erstes empirisches Feedback zur didaktischen Gestaltung zukünftiger Trainingsformate zu gewinnen. Der Vormittag diente der Einführung in zentrale Konzepte der Incident Response. Dabei erhielten die Teilnehmenden einen Überblick über typische Phasen eines Sicherheitsvorfalls sowie über grundlegende Vorgehensweisen bei der Analyse und Bearbeitung von Cyberangriffen. Zugleich wurden sie mit der im weiteren Verlauf eingesetzten Trainingsumgebung vertraut gemacht.

Am Nachmittag wurden drei unterschiedliche Angriffsszenarien bearbeitet, darunter ein Website-Defacement-Szenario, ein Phishing- bzw. Data-Leak-Szenario sowie ein Szenario mit Remote Code Execution. Die Teilnehmenden analysierten die jeweiligen Angriffsabläufe und reflektierten

mögliche Reaktionsmaßnahmen. Die Übung diente damit in erster Linie der Erhebung eines ersten Bildes über Vorkenntnisse, Erwartungen und Interessen der Zielgruppe und bildete eine wesentliche Grundlage für die nachfolgende curriculare Ausdifferenzierung.

6.3.1.2 Evaluierungsergebnisse

Die Vorab-Erhebung unter den 20 Teilnehmenden zeichnete ein differenziertes Bild der Ausgangssituation. Hinsichtlich der Vorkenntnisse erwies sich die Gruppe als deutlich heterogen: Etwa die Hälfte der Teilnehmenden verfügte bereits über Erfahrungen im Bereich Cybersecurity, während die andere Hälfte eher als Einsteigergruppe einzuordnen war. Das formale Bildungsniveau war überwiegend durch Matura geprägt, vereinzelt lagen Pflichtschul- oder Lehrabschlüsse vor. Als zentrale Motivationsfaktoren wurden insbesondere der Wunsch nach praktischen Fähigkeiten, ein gesteigertes Sicherheitsbewusstsein sowie Neugier und Interesse an analytischem Denken genannt.

Inhaltlich zeigten sich starke Interessen in den Bereichen System- und Netzwerksicherheit, SIEM, Threat Hunting und Offensive Security, während Themen wie ICS-Sicherheit oder Cyber-Kriegsführung eine geringere Resonanz fanden. Als besonders relevante Bedrohungen wurden Ransomware, Phishing, Malware und Cyber-Spionage benannt. Gleichzeitig zeigte sich, dass Grundbegriffe wie die CIA-Triad zwar weitgehend bekannt waren, bei Normen und Frameworks wie COBIT, ITIL, IEC 62443 oder CIS Controls jedoch deutliche Wissenslücken bestanden. In didaktischer Hinsicht sprach sich die Gruppe klar für praxisorientierte Prüfungs- und Lernformate aus und formulierte zugleich Erwartungen an fachlich kompetente, praxiserfahrene und feedbackorientierte Trainerinnen und Trainer.

Auch die Bewertung der praktischen Übungsphase fiel insgesamt positiv aus. Die Veranstaltung wurde überwiegend als lernförderlich wahrgenommen, wenngleich der Schwierigkeitsgrad durchgehend als hoch oder sehr hoch eingeschätzt wurde. Diese Einschätzung ist insbesondere vor dem Hintergrund der fehlenden SIEM-Vorerfahrungen der Teilnehmenden plausibel. Hinzu kam, dass auch die Linux-Kenntnisse überwiegend im unteren bis mittleren Bereich lagen. Gleichwohl berichtete die Mehrheit von einem spürbaren Lerngewinn. Die Teamarbeit wurde überwiegend positiv beurteilt, auch wenn die Teilnehmenden ihren eigenen Beitrag teils eher zurückhaltend einschätzten. Insgesamt ließ sich eine hohe Offenheit gegenüber der Integration von Cyberübungen in die reguläre Ausbildung feststellen.

Das qualitative Feedback verdeutlichte zugleich mehrere Entwicklungsbedarfe. Kritisch hervorgehoben wurden insbesondere die begrenzte Eignung des Formats für Personen ohne SIEM-Vorerfahrung, der Wunsch nach einer stärkeren theoretischen Vorbereitung sowie der Bedarf an einem strukturierteren Onboarding. Insgesamt bestätigte die Übung zwar die Relevanz realistischer Angriffsszenarien als motivierendes Lernformat, machte jedoch ebenso deutlich, dass die Anschlussfähigkeit an heterogene Eingangsvoraussetzungen didaktisch noch stärker berücksichtigt werden muss.

6.3.1.3 Zentrale Erkenntnisse für die Weiterentwicklung

Aus der ersten Übung ließen sich mehrere grundlegende Schlussfolgerungen für die Weiterentwicklung des Ausbildungsprogramms ableiten. Erstens zeigte sich, dass dedizierte Einführungsmodule zu SIEM-Systemen und Linux-Grundlagen vor anspruchsvolleren praktischen Übungsformaten erforderlich sind, um die Einstiegshürde zu reduzieren. Zweitens wurde deutlich, dass die Heterogenität der Zielgruppe eine stärkere curriculare Differenzierung notwendig macht. Gestufte Lernpfade sind erforderlich, um sowohl Teilnehmende mit geringen Vorkenntnissen als auch fortgeschrittene Personen angemessen anzusprechen.

Drittens wurde sichtbar, dass bestehende Wissenslücken im Bereich relevanter Normen und Frameworks curricular expliziter aufgegriffen werden sollten. Zugleich bestätigte die Übung zwei zentrale Grundannahmen des Projekts: Zum einen besteht eine deutliche Präferenz der Zielgruppe für praktische Übungs- und Prüfungsformate, zum anderen werden realistische Angriffsszenarien als besonders relevant und motivierend wahrgenommen. Die erste Übung hatte damit primär explorativen Charakter und lieferte wesentliche Hinweise für die anschließende didaktische und curriculare Nachschärfung.

6.3.2 Zweite Cyber-Übung September 2024

Mit der zweiten Cyber-Übung trat das Projekt in eine Phase ein, in der nicht mehr primär grundlegende Bedarfe erhoben, sondern bereits entwickelte curriculare Module unter realitätsnahen Bedingungen erprobt wurden. Die Übung markiert damit einen wichtigen Übergang von der initialen Exploration hin zur systematischeren Prüfung konkreter Ausbildungsinhalte und didaktischer Formate. Zugleich erwies sich diese Veranstaltung als besonders aufschlussreich für die Frage, in welchem Verhältnis theoretische Wissensvermittlung und praktische Anwendung in einem wirksamen Trainingsdesign zueinander stehen sollten. Die nachfolgenden Unterabschnitte rekonstruieren das Übungskonzept, analysieren die Evaluierungsergebnisse und zeigen, warum die zweite Übung einen entscheidenden Impuls für die spätere Neuausrichtung des didaktischen Ansatzes lieferte.

6.3.2.1 Übungskonzept und Zielsetzung

Die zweite Cyber-Übung fand am 19. und 20. September 2024 am AIT in Wien statt und markierte den Meilenstein M 5.2 des Projekts. An der zweitägigen Veranstaltung nahmen 18 Personen teil, darunter 15 Soldaten des fünften Semesters der Militärakademie sowie drei Personen der Führungsunterstützungsschule. Ziel der Übung war es, erstmals mehrere konkrete Ausbildungsmodule aus dem entwickelten Curriculum in einem zusammenhängenden Trainingsformat zu erproben.

Im Unterschied zur ersten Übung stand nun weniger die initiale Bedarfserhebung als vielmehr die systematische Erprobung curricular ausformulierter Themenbereiche im Mittelpunkt. Jedes Modul verband eine theoretische Einführung mit einer praktischen Übungseinheit, um konzeptionelle Grundlagen und erste Anwendungskompetenzen zu vermitteln. Der erste Trainingstag umfasste grundlegende Themenfelder wie IT- und OT-Sicherheit, Open Source Intelligence, Threat Analysis und Netzwerksicherheit. Der zweite Tag fokussierte stärker auf technische Analyse- und Reaktionsmethoden, insbesondere Schwachstellenanalysen, Kommunikationsprotokolle, Incident Response und digitale Forensik.

Die Übung war damit so angelegt, dass ein breiter Ausschnitt des Curriculums praktisch getestet werden konnte. Zugleich sollte überprüft werden, in welchem Verhältnis theoretische Vermittlung und praktische Anwendung für die Zielgruppe als lernwirksam und anschlussfähig erlebt werden.

6.3.2.2 Evaluierungsergebnisse

Die Evaluierung zeigte zunächst eine solide Beteiligung am ersten Tag, während die Rücklaufquote am zweiten Tag deutlich geringer ausfiel. Dies deutet auf mögliche Ermüdungseffekte oder organisatorische Einflussfaktoren hin und ist bei der Interpretation der Ergebnisse zu berücksichtigen. Inhaltlich wurden die einzelnen Module unterschiedlich bewertet, wobei sich insgesamt ein konsistentes Muster erkennen lässt.

Das Einstiegsmodul zu IT- und OT-Sicherheit wurde grundsätzlich als geeignete Grundlage wahrgenommen, zugleich aber von einem Teil der Gruppe als noch vertiefungsfähig eingeschätzt. Beim OSINT-Modul wurden die theoretischen Grundlagen als solide bewertet, während

insbesondere der Wunsch nach intensiveren praktischen Übungsanteilen deutlich wurde. Die Schwachstellenanalyse machte die Heterogenität der Zielgruppe besonders sichtbar, da die Bewertungen stark entlang der unterschiedlichen Vorkenntnisse variierten.

Besonders positiv hervorgehoben wurde das Modul zu Kommunikationsprotokollen. Die darin enthaltene Wireshark-Übung wurde mehrfach als gelungenes Beispiel einer überzeugenden Theorie-Praxis-Verknüpfung genannt. Auch das Modul Threat Analysis wurde inhaltlich als angemessen beurteilt, wobei ebenfalls ein stärkerer praktischer Bezug gewünscht wurde. Netzwerksicherheit erwies sich für einen Teil der Gruppe als besonders anspruchsvoll und machte damit den Bedarf einer gezielteren Vorbereitung sichtbar. Das Incident-Response-Modul wurde demgegenüber überwiegend als stimmig und gut austariert wahrgenommen. Bei der forensischen Analyse zeigte sich, dass eine ausführlichere theoretische Einführung den Übergang in die praktische Anwendung erleichtert hätte.

Über die Einzelmodule hinaus ergab sich ein deutliches Gesamtbild: Der Theorieanteil wurde von vielen Teilnehmenden als zu hoch empfunden, während die als Übungen angekündigten Einheiten teilweise nicht als ausreichend handlungsorientiert erlebt wurden. Mehrfach wurde angemerkt, dass der Charakter der Veranstaltung eher an eine klassische Lehrveranstaltung erinnere und das Potential der Cyber Range noch nicht konsequent ausgeschöpft werde. Zugleich wurden Organisation, Atmosphäre und Rahmenbedingungen positiv bewertet, und die Bereitschaft zu einer erneuten Teilnahme war hoch.

6.3.2.3 Zentrale Erkenntnisse für die Weiterentwicklung

Die zweite Übung markierte einen entscheidenden Wendepunkt im didaktischen Entwicklungsprozess des Projekts. Die Rückmeldungen machten deutlich, dass eine bloße Kombination aus theoretischen Inputs und nachgelagerten Übungselementen nicht ausreicht, um die gewünschte Praxisnähe und Handlungskompetenz systematisch zu fördern. Insbesondere die Diskrepanz zwischen vergleichsweise allgemeiner Theorie und anschließend sehr spezifischer, teils wenig angeleiteter Praxis wurde als problematisch wahrgenommen.

Für die Weiterentwicklung des Ausbildungsformats ergab sich daraus die Notwendigkeit eines grundlegenden didaktischen Paradigmenwechsels. Künftig sollte nicht mehr eine lehrveranstaltungsähnliche Struktur mit ergänzenden Übungen im Vordergrund stehen, sondern ein zusammenhängendes praktisches Projekt bzw. Szenario, in das theoretische Impulse gezielt und situationsbezogen eingebettet werden. Daraus leitete sich die Zielsetzung ab, das Verhältnis von Theorie und Praxis deutlich zugunsten praktischer Anwendungsphasen zu verschieben und theoretische Inputs stärker nach dem Just-in-Time-Prinzip direkt vor der jeweiligen Anwendung zu platzieren.

Zugleich wurde deutlich, dass zukünftige Übungseinheiten konsequent an realen Tools, Systemen und konkreten Aufgabenstellungen ausgerichtet sein müssen. Die Wireshark-Übung erwies sich in diesem Zusammenhang als prototypisch für ein Format, das von der Zielgruppe als besonders lernwirksam wahrgenommen wurde. Die zweite Übung lieferte damit den entscheidenden empirischen Impuls für die spätere stärkere Szenario- und Praxisorientierung des Curriculums.

6.3.3 Dritte Cyber-Übung Juli 2025

Die dritte Cyber-Übung ist vor dem Hintergrund der in der zweiten Übung gewonnenen Erkenntnisse zu lesen und stellt die erste umfassende Umsetzung des überarbeiteten didaktischen Ansatzes dar. Im Zentrum stand nun ein deutlich stärker praxis- und szenariobasierter Zugang, der die Teilnehmenden nicht mehr nur punktuell mit einzelnen Themenmodulen konfrontierte, sondern sie in einen zusammenhängenden Lern- und Anwendungskontext einband. Damit kommt dieser Übung eine besondere Bedeutung zu, da sie erstmals belastbar erkennen lässt, inwiefern das

überarbeitete Format die angestrebte Verbindung von Fachwissen, Handlungskompetenz und Teamarbeit tatsächlich unterstützt. Die folgenden Unterabschnitte beschreiben das Übungskonzept, ordnen die Evaluierungsergebnisse ein und leiten daraus die zentralen Konsequenzen für die weitere Ausgestaltung des Curriculums und der Trainingsumgebung ab.

6.3.3.1 Übungskonzept und Zielsetzung

Die dritte Cyber-Übung fand vom 15. bis 17. Juli 2025 am AIT in Wien statt und setzte die aus den vorangegangenen Übungen gewonnenen Erkenntnisse in ein grundlegend überarbeitetes Trainingsformat um. An der Veranstaltung nahmen 18 Soldaten der Militärakademie sowie drei Personen der Führungsunterstützungsschule teil. Da es sich um dieselbe Zielgruppe wie bei der zweiten Übung handelte, ergab sich eine besonders günstige Ausgangslage für einen Vergleich der Wirkungen des veränderten didaktischen Ansatzes.

Im Zentrum stand nun ein deutlich stärkerer Praxisbezug. Die Inhalte wurden szenariobasiert aufgebaut und in eine umfassende Cyber-Range-Übung überführt, in der ein realistischer Cyberangriff analysiert werden musste. Der erste Trainingstag fokussierte auf Threat Intelligence, die Erstellung eines Situational Picture und die Analyse typischer Verhaltensmuster von Angreifern. Der zweite Tag konzentrierte sich auf Anomaly Detection, Log-Analyse, Grundlagen von SIEM-Technologien und die Einführung in das spätere Übungsszenario. Der dritte Tag war vollständig der praktischen Cyber-Range-Übung gewidmet.

Mit dieser Struktur wurde ein Lernsetting geschaffen, das nicht nur einzelne Module abprüfte, sondern die Teilnehmenden schrittweise in ein zusammenhängendes Anwendungsszenario überführte. Damit rückte die Frage in den Vordergrund, inwiefern ein stärker praxisorientiertes und szenariobasiertes Format den Lernerfolg, die Motivation und die Teamarbeit verbessern kann.

6.3.3.2 Evaluierungsergebnisse

Die dritte Übung stellte im Vergleich zu den vorangegangenen Veranstaltungen deutlich höhere Anforderungen an die Teilnehmenden. Das erhöhte Praxisniveau und das durchgehend szenariobasierte Format wurden grundsätzlich positiv bewertet, erwiesen sich jedoch zugleich als anspruchsvoll. Insbesondere die abschließende Cyber-Range-Übung verlangte den Teilnehmenden ein hohes Maß an technischem Verständnis, analytischer Strukturierung und Zusammenarbeit unter Zeitdruck ab. Der beobachtbare Lerneffekt war deutlich, zugleich wurde sichtbar, dass eine gezieltere Vorbereitung auf die eingesetzten Tools und die Trainingsumgebung den Zugang zum Szenario weiter erleichtert hätte.

Das Einstiegsmodul Threat Intelligence wurde insgesamt positiv aufgenommen. Besonders die Demonstration des Tools Taranis wurde als anschaulicher Zugang zur praktischen Anwendung von OSINT und Threat-Intelligence-Konzepten wahrgenommen. Auch das Modul Situational Picture erwies sich als anschlussfähig: Die gemeinsame Erstellung eines Lagebilds im Rahmen einer Tabletop-Übung förderte Diskussion, Gruppenarbeit und die Übertragung theoretischer Konzepte in einen realitätsnahen Kontext.

Ebenso positiv wurden die Module Anomaly Detection und Log Analysis bewertet. Die Verbindung von theoretischer Einführung und praktischer Aufgabenbearbeitung erwies sich hier als gut austariert. Beim Modul Fundamentals of SIEM Technology wurde hingegen mehrfach angemerkt, dass die Einführung in Kibana als zentrales Werkzeug zu knapp ausgefallen sei. Gerade für Teilnehmende ohne Vorerfahrung stellte dies eine nicht zu unterschätzende Hürde dar. Ähnliches galt für die Vorstellung der Cyber-Range-Infrastruktur, die zwar als notwendige Brücke zum Szenario wahrgenommen wurde, jedoch eine längere Einarbeitungsphase sinnvoll erscheinen ließ.

Die abschließende Cyber-Range-Übung bildete den inhaltlichen Schwerpunkt der Veranstaltung. Die Aufgabe, als fiktives Unternehmen einen simulierten Angriff mithilfe von Kibana eigenständig zu analysieren und zu rekonstruieren, wurde als anspruchsvoll, aber zugleich besonders lernwirksam erlebt. Auffällig war, dass die Teamarbeit in dieser Übung besser funktionierte als in den vorherigen Formaten. Die gemeinsame Nachbesprechung und schrittweise Auflösung des Angriffsszenarios wurde von den Teilnehmenden als besonders wertvoll hervorgehoben, da sie half, eigene Analysen einzuordnen und das Gesamtbild des Vorfalls nachzuvollziehen.

6.3.3.3 Zentrale Erkenntnisse für die Weiterentwicklung

Die dritte Übung bestätigte die Zweckmäßigkeit des eingeschlagenen Weges hin zu einer stärkeren Praxis- und Szenarioorientierung. Das durchgehende Cyber-Range-Szenario erwies sich als besonders wirkungsvolles Format, das Motivation, Teamarbeit und Kompetenzaufbau in produktiver Weise miteinander verknüpfte. Damit wurde empirisch gestützt, dass eine stärker an realitätsnahen Handlungssituationen orientierte Ausbildung dem zuvor verfolgten stärker lehrveranstaltungsformigen Ansatz überlegen ist.

Gleichzeitig machte die Übung deutlich, dass die Wirksamkeit solcher Szenarien wesentlich von der vorgelagerten Werkzeug- und Umgebungsorientierung abhängt. Insbesondere für Analysewerkzeuge wie Kibana ist eine ausreichend umfangreiche, geführte Einführung notwendig, damit die kognitive Belastung in der eigentlichen Übung auf die fachliche Problembearbeitung und nicht primär auf die Bedienung des Tools entfällt. Gleiches gilt für die Einführung in die Struktur und Logik der simulierten Infrastruktur. Die aus der dritten Übung abgeleiteten Optimierungsbedarfe betrafen daher weniger die grundsätzliche Architektur des Formats als vielmehr die zeitliche und didaktische Dosierung der vorbereitenden Phasen.

6.3.4 Vierte Cyber-Übung März 2026

Die vierte Cyber-Übung bildet den abschließenden empirischen Validierungsschritt des im Projekt Bumblebee entwickelten Ausbildungsansatzes. Während die vorangegangenen Übungen vor allem der iterativen Erprobung und Optimierung einzelner curricularer, didaktischer und technischer Elemente dienten, stand nun die zusammenhängende Prüfung des weiterentwickelten Gesamtformats im Vordergrund. Der Abschnitt ist daher als abschließende Verdichtung der im Projektverlauf gewonnenen Erkenntnisse zu verstehen: Er zeigt, inwiefern das entwickelte Curriculum, die Trainingsunterlagen und die technische Trainingsumgebung in ihrer finalen Ausprägung unter realitätsnahen Bedingungen tragfähig sind. Die nachfolgenden Unterabschnitte beschreiben das Übungskonzept, analysieren die Evaluierungsergebnisse und verdichten die daraus ableitbaren Schlussfolgerungen für die abschließende Bewertung des Ausbildungsprogramms.

6.3.4.1 Übungskonzept und Zielsetzung

Die vierte Cyber-Übung fand vom 09. bis 13. März 2026 in Zusammenarbeit mit der Führungsunterstützungsschule statt und bildete die abschließende Demonstrations- und Validierungsphase des Projekts Bumblebee im Rahmen des Arbeitspakets 5. Ziel der fünftägigen Veranstaltung war es, das im Projekt entwickelte Curriculum sowie die dazugehörigen Trainingsunterlagen unter realitätsnahen Bedingungen abschließend zu testen und zu evaluieren.

Im Unterschied zu den vorhergehenden Übungen wurde die Veranstaltung als durchgehendes, mehrtägiges Trainingsprogramm konzipiert, das verschiedene zentrale Bereiche der Cybersecurity-Ausbildung in einem kohärenten Lernprozess miteinander verband. Neben technischen Analysefähigkeiten standen auch methodische Aspekte der Incident Response, die Arbeit in Teams sowie die Nutzung unterschiedlicher Werkzeuge und Trainingsumgebungen im Fokus. Der erste Trainingstag widmete sich grundlegenden Bedrohungskonzepten und

Angreiferperspektiven, einschließlich praktischer Übungen auf der Plattform Hack-the-Box. Der zweite Tag fokussierte auf IT-Forensik und OSINT. Am dritten Tag standen Incident Response, CSIRT-Arbeitsweisen, Eskalationslogiken und strukturierte Lageberichterstattung im Mittelpunkt. Der vierte Tag diente der gezielten Vorbereitung auf die abschließende Cyber-Range-Übung, insbesondere durch die Einführung in Infrastruktur, Datenquellen und SIEM-gestützte Analysewerkzeuge. Der fünfte Trainingstag war schließlich vollständig der Analyse eines simulierten Cyberangriffs in der Cyber Range gewidmet.

Diese mehrtägige Anlage ermöglichte einen didaktisch kohärenten Aufbau, in dem die Teilnehmenden schrittweise von grundlegenden Konzepten über Analyse- und Forensikmethoden bis hin zur eigenständigen Incident-Response-Arbeit in einer realitätsnahen Trainingsumgebung geführt wurden.

6.3.4.2 Evaluierungsergebnisse

An der Abschlussevaluierung beteiligten sich 26 Teilnehmende, sodass für die finale Validierung des Curriculums eine vergleichsweise breite empirische Basis zur Verfügung stand. Die Gruppe war hinsichtlich ihrer Vorkenntnisse heterogen zusammengesetzt und umfasste sowohl Personen mit geringer oder fehlender Vorerfahrung als auch Teilnehmende mit mittlerem und fortgeschrittenem Kenntnisstand. Insgesamt fiel die Bewertung der Veranstaltung deutlich positiv aus; insbesondere die abschließende Cyber-Range-Übung wurde als besonders lernwirksames und authentisches Format hervorgehoben.

Der erste Trainingstag, der Cyber Threats und Hack-the-Box kombinierte, wurde als geeigneter Einstieg in die Woche wahrgenommen. Die Einführung in aktuelle Bedrohungslagen und die Cyber Kill Chain schuf eine tragfähige konzeptionelle Grundlage. Die praktischen Übungen auf der Plattform Hack-the-Box wurden als motivierend und praxisnah beschrieben, wenngleich für Teilnehmende ohne Vorerfahrung eine noch stärker begleitete Einführung in die verwendeten Tools wünschenswert erschien.

Auch das Modul IT-Forensik wurde überwiegend positiv bewertet. Die praktische Analyse digitaler Artefakte erwies sich als anschlussfähig und lernwirksam. Beim OSINT-Teil zeigte sich erneut, dass eine stärkere Einbettung realer Rechercheaufgaben und offener Quellen die Authentizität und Praxisnähe des Moduls weiter erhöhen könnte. Die Ergebnispräsentationen am Ende des Tages wurden als strukturierendes und reflektierendes Element positiv beurteilt.

Das Modul Incident Response und CSIRT-Arbeitsweisen wurde inhaltlich als hoch relevant eingeschätzt. Die Tabletop-Übung, die Arbeit an Eskalationsplänen und Kommunikationsmatrizen sowie das SITREP-Training wurden als praxisnahe Formate wahrgenommen, die den Bezug zu realen Abläufen in besonderer Weise verdeutlichten. Vereinzelt wurde angeregt, Aufgabenstellungen stärker zu kleinschrittigen Lernsequenzen auszubauen, um insbesondere Teilnehmende mit geringeren Vorkenntnissen noch gezielter zu unterstützen.

Der vierte Tag erfüllte seine Funktion als vorbereitende Brücke zur abschließenden Cyber-Range-Übung in überzeugender Weise. Besonders die geführte Einführung in Kibana und das Elastic-SIEM wurde als relevant und hilfreich beurteilt. Im Vergleich zur dritten Übung zeigte sich hier eine deutliche Verbesserung hinsichtlich der Werkzeugorientierung und der Anschlussfähigkeit an das spätere Szenario.

Die Cyber-Range-Übung am fünften Tag bildete den unbestrittenen Schwerpunkt der gesamten Veranstaltung. In Teams analysierten die Teilnehmenden einen simulierten Cyberangriff mit mehreren parallel verlaufenden Angriffsvektoren. Dabei wurden sowohl die Authentizität des Szenarios als auch die Qualität der gemeinsamen Nachbesprechung besonders hervorgehoben. Die Übung vermittelte nach Aussage vieler Teilnehmender ein realistisches Bild davon, wie Incident

Response in einem komplexeren organisationsnahen Umfeld ablaufen kann. Auch Teamkoordination und Rollenverteilung wurden als funktional und lernförderlich beschrieben.

6.3.4.3 Zentrale Erkenntnisse für die Weiterentwicklung

Die vierte Übung bestätigte in verdichteter Form, dass das im Projektverlauf überarbeitete Curriculum mit seinem starken Praxisfokus und dem mehrtägigen szenariobasierten Aufbau eine tragfähige Grundlage für zukünftige Ausbildungsformate im militärischen Cyberkontext darstellt. Besonders die Cyber-Range-Übung erwies sich erneut als das didaktisch wirksamste Element des Gesamtformats und sollte daher als zentraler Bestandteil künftiger Trainings beibehalten werden.

Ebenso wurde bestätigt, dass die mehrtägige Struktur, in der Teilnehmende schrittweise von grundlegenden Konzepten über Analyse- und Forensikmethoden zur eigenständigen Bearbeitung komplexerer Vorfälle geführt werden, als kohärenter Lernprozess wahrgenommen wird. Die gezielte Vorbereitung auf Analysewerkzeuge und Trainingsinfrastruktur zeigte eine deutlich positive Wirkung und reduzierte erkennbare Einstiegshürden in die komplexeren Anwendungsszenarien.

Weiterer Optimierungsbedarf zeigte sich vor allem im Bereich OSINT, wo eine stärkere Einbindung realer Rechercheumgebungen und offener Quellen die Praxisnähe des Moduls erhöhen könnte. Darüber hinaus legen die Rückmeldungen nahe, Aufgabenstellungen für weniger erfahrene Teilnehmende teilweise stärker zu strukturieren, um den schrittweisen Kompetenzaufbau noch gezielter zu unterstützen. Insgesamt bestätigen die Ergebnisse jedoch, dass das entwickelte Curriculum und die zugehörigen Trainingsunterlagen unter realitätsnahen Bedingungen funktionieren, von der Zielgruppe als relevant wahrgenommen werden und einen belastbaren Rahmen für die weitere Verstetigung der Ausbildung bilden.

7 Zusammenfassung und Conclusio

Die Zusammenführung der vier zentralen Berichtsteile macht die konzeptionelle Geschlossenheit des Projekts Bumblebee besonders deutlich. Die Bedarfsanalyse identifiziert die Anforderungen eines militärischen Ausbildungsprogramms für den Cyber- und Informationsraum als mehrdimensionales Gefüge aus technischen, organisatorischen, prozessualen und didaktischen Bedingungen. Auf dieser Grundlage wird mit dem Konzept der Trainingsumgebung ein technischer Rahmen entwickelt, der Reproduzierbarkeit, Sicherheit, Beobachtbarkeit und Integrationsfähigkeit systematisch adressiert. Das Curriculum übersetzt diese Voraussetzungen in eine strukturierte Ausbildungsarchitektur, die gemeinsames Grundlagenwissen, rollenbezogene Spezialisierung und praxisnahe Anwendung miteinander verbindet. Die Evaluierung der durchgeführten Trainings belegt schließlich, dass diese Architektur nicht nur theoretisch konsistent, sondern auch praktisch anschlussfähig ist.

In wissenschaftlicher Perspektive zeigt der Endbericht, dass wirksame Cyber-Ausbildung in militärischen Kontexten nicht als isolierte Technologie- oder Toolschulung verstanden werden kann. Sie erfordert vielmehr die konsequente Verbindung von Anforderungsanalyse, technischer Infrastruktur, didaktischer Progression und empirischer Rückkopplung. Gerade die im Projekt vollzogene Verschränkung dieser Ebenen stellt einen zentralen Mehrwert dar. Das Vorhaben entwickelt damit keinen singulären Lehrgang, sondern einen belastbaren Referenzrahmen für die institutionalisierte Entwicklung militärischer Cyber-Ausbildungsfähigkeit.

Besonders hervorzuheben ist die Rolle der Trainingsumgebung als Bindeglied zwischen Bedarfsanalyse und Curriculum. Die technische Plattform wird im Projekt nicht als nachgelagerte Betriebsfrage behandelt, sondern als didaktisch wirksame Voraussetzung der Ausbildung. Reproduzierbare Szenarien, sichere Isolierung, förderbare Übungsumgebungen, strukturierte Telemetrie und After-Action-Review-Fähigkeiten sind nicht nur technische Merkmale, sondern Bedingungen dafür, dass Lernen unter realitätsnahen, kontrollierbaren und evaluierbaren Umständen stattfinden kann. Damit wird deutlich, dass Architekturentscheidungen und curriculare Entscheidungen im militärischen Cyberbereich nicht voneinander getrennt betrachtet werden können.

Ebenso zeigt sich, dass die Qualität des Curriculums wesentlich von seiner Rückbindung an reale Übungs- und Evaluierungserfahrungen abhängt. Die dokumentierten Trainings verdeutlichen, dass heterogene Vorkenntnisse, differenzierte Zielgruppenbedarfe und die Balance zwischen Theorie, Guided Labs und komplexen Übungsszenarien in iterativen Zyklen bearbeitet werden müssen. Die empirische Validierung stärkt damit nicht nur die Glaubwürdigkeit des entwickelten Ausbildungsansatzes, sondern liefert zugleich einen Mechanismus für seine fortlaufende Verbesserung. Das Projekt hat auf diese Weise einen evidenzbasierten Entwicklungsprozess etabliert, der curriculare Weiterentwicklung, Plattformgestaltung und Trainingspraxis eng miteinander verknüpft.

In der Gesamtschau lässt sich festhalten, dass Bumblebee eine tragfähige Grundlage für die weitere Institutionalisierung militärischer Cyber-Ausbildung geschaffen hat. Der Endbericht dokumentiert nicht nur Ergebnisse, sondern ein konsistentes Entwicklungsmodell: Bedarfe werden systematisch erhoben, in technische und curriculare Entscheidungen überführt, praktisch erprobt und anhand evaluativer Rückkopplung weiterentwickelt. Damit entsteht ein Rahmen, der sowohl für die zukünftige Aus- und Fortbildung militärischen Personals als auch für die strategische Weiterentwicklung entsprechender Fähigkeiten im Cyber- und Informationsraum von substanziellem Wert ist.



8 Literaturverzeichnis

- [1] "Cyberaggression: Hybride Bedrohungen des 21. Jahrhunderts und wie wir uns vor ihnen schützen," Bundesamt für Sicherheit in der Informationstechnik. Accessed: Mar. 17, 2026. [Online]. Available: https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Blog/Cyberaggression_250216.html?nn=520690
- [2] M. Glas, M. Vielberth, and G. Pernul, "Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges," in Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, in CHI '23. New York, NY, USA: Association for Computing Machinery, Apr. 2023, pp. 1–19. doi: 10.1145/3544548.3581046.
- [3] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. 2020. Accessed: Mar. 17, 2026. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020JC0018>
- [4] "ENISA Threat Landscape 2024 | ENISA." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- [5] "Standardization," Site name seo. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.nato.int/en/what-we-do/deterrence-and-defence/standardization>
- [6] "ISO/IEC 27001:2022," ISO. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.iso.org/standard/27001>
- [7] "COBIT® | Control Objectives for Information Technologies®," ISACA. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.isaca.org/resources/cobit>
- [8] "Welcome to ITIL." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.itil.com/>
- [9] "ISA/IEC 62443 Series of Standards - ISA," isa.org. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
- [10] "CIS Critical Security Controls Version 8." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.cisecurity.org/controls/v8>
- [11] T. GmbH, "Ausbildung zum IKT-Offizier." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.milak.at/ikt-offizier/ausbildung>
- [12] "Bundesheer - Cyber-Kräfte - Führungsunterstützungsschule." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.bmlv.gv.at/sk/cyber/fueus.shtml>
- [13] "Cyber- und Informationsraum." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum>
- [14] "Master Cyber-Sicherheit," BND. Accessed: Mar. 17, 2026. [Online]. Available: https://www.bnd.bund.de/DE/Karriere/Ausbildung_Studium/Master/Cyber-Security/master_node_cyber.html
- [15] "Seite 2: Passgenaue Ausbildung | heise online." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.heise.de/news/Duales-Studium-Cyber-Security-hausgemachte-Experten-4659151.html?seite=2>
- [16] E. Toome, "Cybersecurity education: Estonian innovative solution for IT students," Education Estonia. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.educationestonia.org/education-cybersecurity-military-service/>
- [17] "Military education," Estonian Defence Forces. Accessed: Mar. 17, 2026. [Online]. Available: <https://mil.ee/en/defence-forces/military-education/>
- [18] "Formations en cyberdéfense | Ministère des Armées et des Anciens combattants." Accessed: Mar. 17, 2026. [Online]. Available: <http://www.defense.gouv.fr/comcyber/nous-rejoindre/nos-carrieres/formations-cyberdefense>
- [19] U. degli S. di Torino, "Guida alla Laurea Magistrale in Scienze Strategiche e Militari (055504)," Scuola Universitaria Interdipartimentale in Scienze Strategiche (SUISS). Accessed: Mar. 17, 2026. [Online]. Available: <https://www.suiss.unito.it/do/home.pl/View?doc=LMSienzeStrategicheMilitari.html>
- [20] "The Norwegian Cyber Defence," Norwegian Armed Forces. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.forsvaret.no/en/organisation/norwegian-cyber-defence>
- [21] "Cyber-Miliz." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.vtg.admin.ch/de/cyber-miliz#ui-collapse-147>



- [22] "Army Cyber & Technology Careers," goarmy.com. Accessed: Mar. 17, 2026. [Online]. Available: <http://www.goarmy.com/content/goarmy/en/careers-and-jobs/specialty-careers/army-cyber.html>
- [23] "Home." Accessed: Mar. 17, 2026. [Online]. Available: <https://cybercoe.army.mil/Home/Schools/Cyber-School/>
- [24] "Cyber Technical College." Accessed: Mar. 17, 2026. [Online]. Available: <https://cybercoe.army.mil/Cyber-Center-of-Excellence/Schools/Cyber-School/Cyber-Technical-College/>
- [25] "U.S. Army Cyber Center of Excellence | UMGC." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.umgc.edu/military-and-veterans/military-college-institution-credit/us-army-cyber-center-of-excellence>
- [26] "Cyber Defense Training," SANS Institute. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.sans.org/cybersecurity-focus-areas/cyber-defense>
- [27] "Cybersecurity for Veterans | NICCS." Accessed: Mar. 17, 2026. [Online]. Available: <https://niccs.cisa.gov/audience/cybersecurity-veterans>
- [28] "Cyber Operator | Canadian Armed Forces." Accessed: Mar. 17, 2026. [Online]. Available: <https://forces.ca/en/career/cyber-operator/>
- [29] R. Abaab, "Cyber Programme of the Royal Military College of Canada." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.rmc-cmr.ca/en/engineering/cyber-programme>
- [30] R. Abaab, "Cyber Professional Military Education." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.rmc-cmr.ca/en/engineering/cyber-PME>
- [31] "Become a Communications Engineer - Royal Signal | Army Jobs." Accessed: Mar. 17, 2026. [Online]. Available: <https://jobs.army.mod.uk/roles/royal-signals/cyber-engineer/>
- [32] "Operator Military Intelligence | Army Jobs." Accessed: Mar. 17, 2026. [Online]. Available: <https://jobs.army.mod.uk/roles/intelligence-corps/operator-military-intelligence/>
- [33] "Operator Technical Intelligence | Army Jobs." Accessed: Mar. 17, 2026. [Online]. Available: <https://jobs.army.mod.uk/roles/intelligence-corps/operator-technical-intelligence/>
- [34] "Electronic Warfare & Signals Intelligence - Royal Signals." Accessed: Mar. 17, 2026. [Online]. Available: <https://jobs.army.mod.uk/roles/royal-signals/electronic-warfare-signals-intelligence/>
- [35] "NATO Standardization Office," Organization | NATO. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.nato.int/en/about-us/organization/nato-structure/nato-standardization-office>
- [36] "Education and training," Site name seo. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.nato.int/en/what-we-do/deterrence-and-defence/education-and-training>
- [37] "ISO/IEC 27000 family," Wikipedia. Jun. 12, 2025. Accessed: Mar. 17, 2026. [Online]. Available: https://en.wikipedia.org/w/index.php?title=ISO/IEC_27000_family&oldid=1295265962
- [38] "ISO - ISO/IEC 27000 family — Information security management," ISO. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.iso.org/standard/iso-iec-27000-family>
- [39] "Integrating ITIL and Cybersecurity Frameworks to Improve Security Governance," EasyVista. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.easyvista.com/blog/integrating-til-and-cybersecurity-frameworks-to-improve-security-governance/>
- [40] "Industry News 2019 Employing COBIT 2019 for Enterprise Governance Strategy." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy>
- [41] "What is COBIT? A framework for alignment and governance," CIO. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html>
- [42] "Home | ENISA." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.enisa.europa.eu/>
- [43] "European Cybersecurity Skills Framework Role Profiles | ENISA." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>
- [44] "Good Practice Guide for Incident Management | ENISA." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management>



- [45] C. Pascoe, S. Quinn, and K. Scarfone, "The NIST Cybersecurity Framework (CSF) 2.0," NIST, Feb. 2024, Accessed: Mar. 17, 2026. [Online]. Available: <https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20>
- [46] "NIST Releases Version 2.0 of Landmark Cybersecurity Framework," NIST, Feb. 2024, Accessed: Mar. 17, 2026. [Online]. Available: <https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework>
- [47] "CyBOK – The Cyber Security Body of Knowledge v1.1." Accessed: Mar. 17, 2026. [Online]. Available: https://www.cybok.org/knowledgebase1_1/
- [48] "CyBOK – The Cyber Security Body of Knowledge at a glance." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.cybok.org/ataglance/>
- [49] A. Martin, A. Rashid, H. Chivers, S. Schneider, E. Lupu, and G. Danezis, "Introduction to CyBOK Knowledge Area Version 1.1.0".
- [50] "What is a cyber range? | IBM." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.ibm.com/think/topics/cyber-range>
- [51] "Cyber Defense Training for Government & Military | Cloud Range." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.cloudrangecyber.com/government-and-military>
- [52] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Computers & Security*, vol. 102, p. 102154, Mar. 2021, doi: 10.1016/j.cose.2020.102154.
- [53] G. Lagorio, M. Ribaud, and A. Armando, "Capture the Flag competitions for Higher Education".
- [54] "Cyber Mastery: Community Inspired. Enterprise Trusted. | Hack The Box." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.hackthebox.com>
- [55] "Learn Cyber Security | TryHackMe Cyber Training," TryHackMe. Accessed: Mar. 17, 2026. [Online]. Available: <https://tryhackme.com/>
- [56] K. C. // Ctf. LLC, "CTFd : The Easiest Capture The Flag Framework," CTFd LLC. Accessed: Mar. 17, 2026. [Online]. Available: <https://ctfd.io/>
- [57] "picoCTF - CMU Cybersecurity Competition." Accessed: Mar. 17, 2026. [Online]. Available: <https://picoctf.org/>
- [58] S. Kucek and M. Leitner, "An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments," *Journal of Network and Computer Applications*, vol. 151, p. 102470, Feb. 2020, doi: 10.1016/j.jnca.2019.102470.
- [59] V. E. Urias, W. M. S. Stout, B. Van Leeuwen, and H. Lin, "Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper," in 2018 International Carnahan Conference on Security Technology (ICCST), Oct. 2018, pp. 1–5. doi: 10.1109/CCST.2018.8585460.
- [60] M. Karjalainen and T. Kokkonen, "Comprehensive Cyber Arena; The Next Generation Cyber Range," in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Sep. 2020, pp. 11–16. doi: 10.1109/EuroSPW51379.2020.00011.
- [61] T. Saito et al., "Development of Cyber Ranges for Operational Technology," in 2023 8th International Conference on Business and Industrial Research (ICBIR), May 2023, pp. 1031–1034. doi: 10.1109/ICBIR57571.2023.10147612.
- [62] "Cyber Range & Cyber Security Solutions · DIATEAM," DIATEAM · Cyber Range & Cyber Solutions. Accessed: Mar. 17, 2026. [Online]. Available: <https://www.diateam.net/>
- [63] "CRATE – Sweden's national cyber training facility." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.foi.se/en/foi/research/cyber/crate—swedens-national-cyber-training-facility.html>
- [64] "Realistic Global Cyber Environment | JYVSECTEC." Accessed: Mar. 17, 2026. [Online]. Available: <https://jyvsectec.fi/en/realistic-global-cyber-environment/>
- [65] "CR14." Accessed: Mar. 17, 2026. [Online]. Available: <https://estonia.ee/defence/grants/cr-14>
- [66] "Cyber Training." Accessed: Mar. 17, 2026. [Online]. Available: <https://cybersecurity.leonardo.com/en/security-cyber/cyber-digital-solutions/cyber-training>
- [67] "Norwegian Cyber Range - NTNU." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.ntnu.edu/ncr>
- [68] "Cyber Range Platform: Real Training Scenarios & Simulations." Accessed: Mar. 17, 2026. [Online]. Available: <https://www.cyberbit.com/product/cyber->



- range/?utm_term=cyberbit&utm_campaign=Brand&utm_source=adwords&utm_medium=ppc&hsa_acc=1799109774&hsa_cam=22788456866&hsa_grp=184829060760&hsa_ad=763504131317&hsa_src=g&hsa_tgt=kwd-399586099094&hsa_kw=cyberbit&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=Cj0KCQjw9-PNBhDfARIsABHN6-1gALethWMEa2fKCmeLNF0pMuq8pvrOKqhErngWglaHh5AEkcFNwAaAqWgEALw_wcB
- [69] "Cyber Range Training: Professionelle IT-Sicherheit." Accessed: Mar. 17, 2026. [Online]. Available: <https://cyberrange.at/>
- [70] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, and M. A. Ferrag, "Cyber Ranges and TestBeds for Education, Training, and Research," *Applied Sciences*, vol. 11, no. 4, p. 1809, Feb. 2021, doi: 10.3390/app11041809.
- [71] "Docker overview." Accessed: Mar. 16, 2026. [Online]. Available: <https://docs.docker.com/get-started/docker-overview/>
- [72] "Overview | Kubernetes." Accessed: Mar. 16, 2026. [Online]. Available: <https://kubernetes.io/docs/concepts/overview/>
- [73] "OpenStack – Open Source Cloud Computing Infrastructure." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.openstack.org/>
- [74] "What is Terraform? | Terraform | HashiCorp Developer." Accessed: Mar. 16, 2026. [Online]. Available: <https://developer.hashicorp.com/terraform/intro>
- [75] "Ansible Documentation." Accessed: Mar. 16, 2026. [Online]. Available: <https://docs.ansible.com/>
- [76] "MITRE Caldera." Accessed: Mar. 16, 2026. [Online]. Available: <https://caldera.mitre.org/>
- [77] "Cyber Range Training Events | CISA." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.cisa.gov/resources-tools/training/cyber-range-training-events>
- [78] "Trainings and exercises | ENISA." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.enisa.europa.eu/topics/skills-and-competences/trainings-and-exercises>
- [79] "Locked Shields | NATO CCDCOE." Accessed: Mar. 16, 2026. [Online]. Available: <https://ccdcoe.org/locked-shields/>
- [80] "Cyber range design framework for cyber security education and training | International Journal of Information Security | Springer Nature Link." Accessed: Mar. 16, 2026. [Online]. Available: <https://link.springer.com/article/10.1007/s10207-023-00680-4>
- [81] "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture | ScienceDirect." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.sciencedirect.com/science/article/abs/pii/S0167404819301804>
- [82] "Exploring the Architectural Composition of Cyber Ranges: A Systematic Review | MDPI." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.mdpi.com/1999-5903/16/7/231>
- [83] "A step-by-step definition of a reference architecture for cyber ranges | ScienceDirect." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2214212624002199>
- [84] "CIS Critical Security Controls Implementation Groups | Center for Internet Security." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.cisecurity.org/controls/implementation-groups>
- [85] "ISO/IEC JTC 1/SC 27 — Information security, cybersecurity and privacy protection | ISO." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.iso.org/committee/45306.html>
- [86] "ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements | ISO." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.iso.org/standard/27001>
- [87] "ISO/IEC 27035-1:2023 — Information technology — Information security incident management — Part 1: Principles and process | ISO." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.iso.org/standard/78973.html>
- [88] "ISO/IEC 27032:2023 — Cybersecurity — Guidelines for Internet security | ISO." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.iso.org/standard/76070.html>
- [89] "ITIL 4 Foundation | PeopleCert." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1/itil-4-foundation-2565>



- [90] "ITIL 4 Practitioner: Incident Management | PeopleCert." Accessed: Mar. 16, 2026. [Online]. Available: <https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1/itil4-practices-incident-management-3684>
- [91] *IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)–Framework and Rules*. doi: 10.1109/IEEESTD.2025.11004567.
- [92] *IEEE Standard for Distributed Interactive Simulation–Application Protocols*. doi: 10.1109/IEEESTD.2012.6387564.
- [93] A. A. Bangash, T. Ge, Z. Zhao, A. Singh, Z. Wang, and B. Adams, "The State of the SBOM Tool Ecosystems: A Comparative Analysis of SPDX and CycloneDX," 2025, *arXiv*. doi: 10.48550/ARXIV.2512.21781.
- [94] *IEEE/ISO/IEC International Standard for Software, systems and enterprise–Architecture description*. doi: 10.1109/IEEESTD.2022.9938446.
- [95] I. Pinkster, B. van de Burgt, D. Janssen, and E. van Veenendaal, *Successful Test Management: An Integral Approach*, 1st ed. 2004. Berlin, Heidelberg: Imprint: Springer, 2004. doi: 10.1007/978-3-540-44735-1.
- [96] R. Wojcik *et al.*, "Attribute-Driven Design (ADD), Version 2.0:," Defense Technical Information Center, Fort Belvoir, VA, Nov. 2006. doi: 10.21236/ADA460414.
- [97] M. Stutz and S. Aier, "Vorgehensmodell zur fachlichen Bewertung serviceorientierter Architekturen".
- [98] Robert Nord *et al.*, "Integrating the Architecture Tradeoff Analysis Method (ATAM) with the Cost Benefit Analysis Method (CBAM)." Dec. 01, 2003. doi: 10.1184/R1/6574613.v1.
- [99] M. Souppaya, K. Scarfone, and D. Dodson, "Secure Software Development Framework (SSDF) version 1.1 : recommendations for mitigating the risk of software vulnerabilities," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-218, Feb. 2022. doi: 10.6028/NIST.SP.800-218.
- [100] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
- [101] A. Van Lamsweerde, "Goal-oriented requirements engineering: a guided tour," in *Proceedings Fifth IEEE International Symposium on Requirements Engineering*, Toronto, Ont., Canada: IEEE Comput. Soc, 2000, pp. 249–262. doi: 10.1109/ISRE.2001.948567.
- [102] H. Bergsteiner, G. C. Avery, and R. Neumann, "Kolb's experiential learning model: critique from a modelling perspective," *Studies in Continuing Education*, vol. 32, no. 1, pp. 29–46, Mar. 2010, doi: 10.1080/01580370903534355.
- [103] M. N. Katsantonis, A. Manikas, I. Mavridis, and D. Gritzalis, "Cyber range design framework for cyber security education and training," *Int. J. Inf. Secur.*, vol. 22, no. 4, pp. 1005–1027, Aug. 2023, doi: 10.1007/s10207-023-00680-4.
- [104] National Initiative for Cybersecurity Education (NICE), "The Cyber Range - A Guide (NIST-NICE) (Draft)." Accessed: Aug. 18, 2022. [Online]. Available: https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf
- [105] M. Glas, M. Vielberth, and G. Pernul, "Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, Hamburg Germany: ACM, Apr. 2023, pp. 1–19. doi: 10.1145/3544548.3581046.
- [106] M. Glas, F. Böhm, F. Schönteich, and G. Pernul, "Cyber Range Exercises: Potentials and Open Challenges for Organizations," in *Human Aspects of Information Security and Assurance*, vol. 674, S. Furnell and N. Clarke, Eds., in IFIP Advances in Information and Communication Technology, vol. 674. , Cham: Springer Nature Switzerland, 2023, pp. 24–35. doi: 10.1007/978-3-031-38530-8_3.
- [107] W. Lazarov *et al.*, "Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education," *Tech Know Learn*, Apr. 2025, doi: 10.1007/s10758-025-09840-y.
- [108] M. M. Yamin and B. Katt, "Modeling and executing cyber security exercise scenarios in cyber ranges," *Computers & Security*, vol. 116, p. 102635, May 2022, doi: 10.1016/j.cose.2022.102635.

- [109] C. E. Hmelo-Silver, "Problem-Based Learning: What and How Do Students Learn?," *Educational Psychology Review*, vol. 16, no. 3, pp. 235–266, Sept. 2004, doi: 10.1023/B:EDPR.0000034022.16470.f3.
- [110] T. Ghosh and G. Francia, "Assessing Competencies Using Scenario-Based Learning in Cybersecurity," *JCP*, vol. 1, no. 4, pp. 539–552, Sept. 2021, doi: 10.3390/jcp1040027.
- [111] R. English, "Designing and Developing a Scenario-Based Curriculum for Cyber Education in HE," in *Cybersecurity Teaching in Higher Education*, L. F. Sikos and P. Haskell-Dowland, Eds., Cham: Springer International Publishing, 2023, pp. 59–77. doi: 10.1007/978-3-031-24216-8_3.
- [112] J. R. Savery, "Overview of Problem-based Learning: Definitions and Distinctions," *Interdisciplinary Journal of Problem-Based Learning*, vol. 1, no. 1, May 2006, doi: 10.7771/1541-5015.1002.
- [113] A. Brilingaitė, L. Bukauskas, and A. Juozapavičius, "A framework for competence development and assessment in hybrid cybersecurity exercises," *Computers & Security*, vol. 88, p. 101607, Jan. 2020, doi: 10.1016/j.cose.2019.101607.
- [114] B. Green, D. Prince, U. Roedig, J. Busby, and D. Hutchison, "Socio-Technical Security Analysis of Industrial Control Systems (ICS)," in *2nd International Symposium for ICS & SCADA Cyber Security Research 2014*, BCS Learning & Development, Sept. 2014. doi: 10.14236/ewic/ics-csr2014.2.
- [115] D. I. Christine and M. Thinyane, "Socio-technical Cyber Resilience: A Systematic Review of Cyber Resilience Management Frameworks," in *Digital Transformation for Sustainability*, J. Marx Gómez and M. R. Lorini, Eds., in Progress in IS., Cham: Springer International Publishing, 2022, pp. 573–597. doi: 10.1007/978-3-031-15420-1_28.
- [116] K. Khadka and A. B. Ullah, "Human factors in cybersecurity: an interdisciplinary review and framework proposal," *Int. J. Inf. Secur.*, vol. 24, no. 3, p. 119, June 2025, doi: 10.1007/s10207-025-01032-0.
- [117] G. Langner, S. Furnell, G. Quirchmayr, and F. Skopik, "A Comprehensive Design Framework for Multi-disciplinary Cyber Security Education," in *Human Aspects of Information Security and Assurance*, vol. 674, S. Furnell and N. Clarke, Eds., in IFIP Advances in Information and Communication Technology, vol. 674., Cham: Springer Nature Switzerland, 2023, pp. 105–115. doi: 10.1007/978-3-031-38530-8_9.
- [118] D. W. Johnson, R. T. Johnson, and M. B. Stanne, "Cooperative Learning Methods: A Meta-Analysis".
- [119] E. Kyndt, E. Raes, B. Lismont, F. Timmers, E. Cascallar, and F. Dochy, "A meta-analysis of the effects of face-to-face cooperative learning. Do recent studies falsify or verify earlier findings?," *Educational Research Review*, vol. 10, pp. 133–149, Dec. 2013, doi: 10.1016/j.edurev.2013.02.002.
- [120] G. Fleming and S. Gillon, "Crisis Resource Management: Training the Responders," in *Textbook of Rapid Response Systems*, M. A. DeVita, Ed., Cham: Springer Nature Switzerland, 2024, pp. 361–368. doi: 10.1007/978-3-031-67951-3_29.
- [121] R. Flin and N. Maran, "Basic concepts for crew resource management and non-technical skills," *Best Practice & Research Clinical Anaesthesiology*, vol. 29, no. 1, pp. 27–39, Mar. 2015, doi: 10.1016/j.bpa.2015.02.002.
- [122] D. W. Johnson, R. T. Johnson, and K. A. Smith, "Cooperative Learning Returns To College What Evidence Is There That It Works?," *Change: The Magazine of Higher Learning*, vol. 30, no. 4, pp. 26–35, July 1998, doi: 10.1080/00091389809602629.
- [123] V. Scarano, P. Giuseppina, J. Andriessen, and M. Pardijs, "Collaborative Cybersecurity Awareness Learning in Higher Education," in *Methodologies and Intelligent Systems for Technology Enhanced Learning, Workshops - 13th International Conference*, vol. 769, Z. Kubincová, F. Caruso, T. Kim, M. Ivanova, L. Lancia, and M. A. Pellegrino, Eds., in Lecture Notes in Networks and Systems, vol. 769., Cham: Springer Nature Switzerland, 2023, pp. 303–312. doi: 10.1007/978-3-031-42134-1_30.
- [124] K. Yoon and S.-Y. Chang, "Teaching Team Collaboration in Cybersecurity: A Case Study from the Transactive Memory Systems Perspective," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, Vienna, Austria: IEEE, Apr. 2021, pp. 841–845. doi: 10.1109/EDUCON46332.2021.9453894.



- [125] A. Seiler and U. Lechner, "Improving Cyber Security Incident Response: A Collaborative Tabletop Game Approach," in *Information Security Education. Empowering People Through Information Security Education*, vol. 742, L. Drevin, W. S. Leung, and S. Von Solms, Eds., in IFIP Advances in Information and Communication Technology, vol. 742, Cham: Springer Nature Switzerland, 2026, pp. 124–139. doi: 10.1007/978-3-031-94924-1_9.
- [126] European Union Agency for Cybersecurity., *ENISA cybersecurity threat landscape methodology*. LU: Publications Office, 2025. Accessed: Dec. 04, 2025. [Online]. Available: <https://data.europa.eu/doi/10.2824/1888892>
- [127] M. Ismail *et al.*, "Cybersecurity activities for education and curriculum design: A survey," *Computers in Human Behavior Reports*, vol. 16, p. 100501, Dec. 2024, doi: 10.1016/j.chbr.2024.100501.
- [128] D. Mouheb, S. Abbas, and M. Merabti, "Cybersecurity Curriculum Design: A Survey," in *Transactions on Edutainment XV*, vol. 11345, Z. Pan, A. D. Cheok, W. Müller, M. Zhang, A. El Rhalibi, and K. Kifayat, Eds., in Lecture Notes in Computer Science, vol. 11345, Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 93–107. doi: 10.1007/978-3-662-59351-6_9.
- [129] M. Mukherjee, N. T. Le, Y.-W. Chow, and W. Susilo, "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," *Information*, vol. 15, no. 2, p. 117, Feb. 2024, doi: 10.3390/info15020117.
- [130] A. J. Blažič and B. J. Blažič, "Toward effective learning of cybersecurity: new curriculum agenda and learning methods," *Journal of Cybersecurity*, vol. 10, no. 1, p. tyae018, Jan. 2024, doi: 10.1093/cybsec/tyae018.
- [131] E. Stavrou, "Planning for Professional Development in Cybersecurity: A New Curriculum Design," in *Human Aspects of Information Security and Assurance*, vol. 674, S. Furnell and N. Clarke, Eds., in IFIP Advances in Information and Communication Technology, vol. 674, Cham: Springer Nature Switzerland, 2023, pp. 91–104. doi: 10.1007/978-3-031-38530-8_8.
- [132] Y. Shin, H. Kwon, J. Jeong, and D. Shin, "A Study on Designing Cyber Training and Cyber Range to Effectively Respond to Cyber Threats," *Electronics*, vol. 13, no. 19, p. 3867, Sept. 2024, doi: 10.3390/electronics13193867.
- [133] M. S. Knowles, E. F. Holton lii, R. A. Swanson, and P. A. Robinson, *The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development*, 9th ed. Routledge, 2020. doi: 10.4324/9780429299612.
- [134] T. Chen, H. Luo, P. Wang, X. Yin, and J. Yang, "The role of pre-class and in-class behaviors in predicting learning performance and experience in flipped classrooms," *Heliyon*, vol. 9, no. 4, p. e15234, Apr. 2023, doi: 10.1016/j.heliyon.2023.e15234.
- [135] G. Wang, "Effects of a Flipped Classroom College Business Course on Students' Pre-Class Preparation, In-Class Participation, Learning, and Skills Development," *Administrative Sciences*, vol. 15, no. 8, p. 301, Aug. 2025, doi: 10.3390/admsci15080301.
- [136] L. Liu, K. F. Hew, and J. Du, "Design principles for supporting self-regulated learning in flipped classrooms: A systematic review," *International Journal of Educational Research*, vol. 124, p. 102319, 2024, doi: 10.1016/j.ijer.2024.102319.
- [137] M. S. Knowles, *Self directed learning: a guide for learners and teachers*, 11. print. New York: Cambridge Adult Education, 2003.
- [138] A. Brilingaitė, L. Bukauskas, and A. Juozapavičius, "A framework for competence development and assessment in hybrid cybersecurity exercises," *Computers & Security*, vol. 88, p. 101607, Jan. 2020, doi: 10.1016/j.cose.2019.101607.
- [139] W. Lazarov *et al.*, "Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education," *Tech Know Learn*, Apr. 2025, doi: 10.1007/s10758-025-09840-y.
- [140] M. Mukherjee, N. T. Le, Y.-W. Chow, and W. Susilo, "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," *Information*, vol. 15, no. 2, p. 117, Feb. 2024, doi: 10.3390/info15020117.
- [141] E. Stavrou, "Planning for Professional Development in Cybersecurity: A New Curriculum Design," in *Human Aspects of Information Security and Assurance*, vol. 674, S. Furnell and N. Clarke, Eds., Cham: Springer Nature Switzerland, 2023, pp. 91–104. doi: 10.1007/978-3-031-38530-8_8.