Bundesministerium
Finanzen

Wissenschaf(f)t Sicherheit

Geförderte KIRAS-Projekte 2019–2021

Wissenschaf(f)t Sicherheit

Geförderte KIRAS-Projekte 2019–2021

Wien, 2023

Impressum

Medieninhaber und Herausgeber:
Bundesministerium für Finanzen Johannesgasse 5, 1010 Wien

Gesamtumsetzung:
Stabsstelle für Sicherheitsforschung und Technologietransfer

Autorinnen und Autoren:
siehe Projektleitung der KIRAS-Projekte

Fotonachweis:
Die Urheberrechte der Fotos liegen bei den jeweiligen Projektträgern
(wenn nicht anders vermerkt)

Gestaltung:
Verlag Holzhausen GmbH, Traungasse 14-16, 1030 Wien.

Produktion:
Bohmann Repromedia und Online GmbH, Rechte Wienzeile 31/Top 1, 1040 Wien

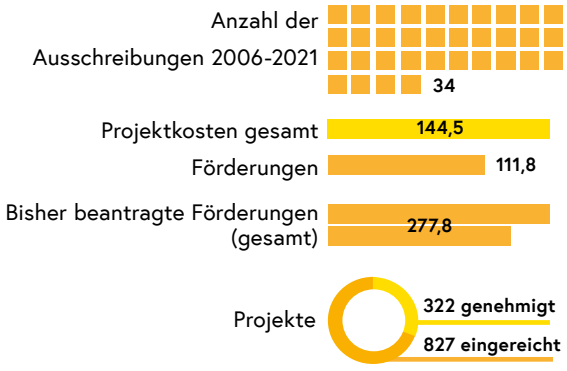
Druck:
KS PRINTSOLUTION, Akazienweg 1, 2542 Kottingbrunn

Bundesministerium Finanzen

KIRAS Sicherheitsforschung

Sicherheitsforschung (national und EU)

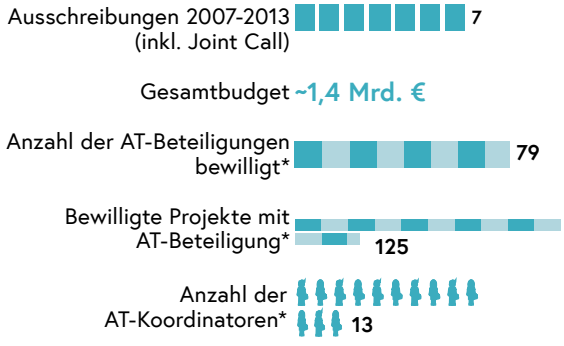
KIRAS www.kiras.at



Bis zum Jahr 2020 erzielte volkswirtschaftliche Effekte (insgesamt 300 Projekte):

- Rund 195,5 Mio. € Wertschöpfungsvolumen bei 103,4 Mio. € Förderbarwert.
- Dabei wurden durch **103,4 Mio. € Projektfördervolumina**, 45,1 Mio. € Sozialversicherungsabgaben und insgesamt zusätzlich **50,4 Mio. € Steuereinnahmen** generiert.
- Mit den KIRAS-Projekten wurden in Österreich bis zum Jahr 2020 über **3.400 Arbeitsplätze** geschaffen bzw. gehalten

ESRP (FP7-SECURITY) http://cordis.europa.eu/



Bis zum Jahr 2014 erzielte volkswirtschaftliche Effekte durch FP7-SECURITY[1]:

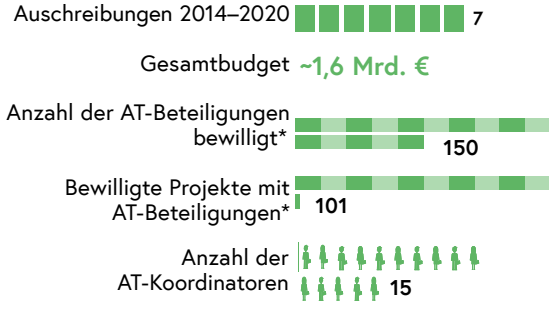
Rund 81, 3 Mio. € Wertschöpfungsvolumen bei 44,3 Mio. € Förderbarwert.

In Östereich wurden mit den FP7-Security-Projekten bis zum Jahr 2014 rund 1.500 Arbeitsplätze geschaffen oder gehalten.

Rückflüsse an AT absolut auf Basis der bewilligten Projekte

44,3 Mio. €

ESRP (H2020 – Secure Societies) http://ec.europa.eu/programmes/horizon2020/h2020-sections



Die österreichische Beteiligung an der europäischen Sicherheitsforschung (FP7-SECURITY wie H2020) zeichnet sich durch überdurchschnittliche **Erfolgs- und Rückflussquoten** aus.

Ein Großteil der in ESRP erfolgreichen österreichischen Teilnehmer konnte auch bereits in KIRAS Erfahrungen sammeln

Dies untermauert die durch KIRAS erreichten Hebeleffekte.

Rückflüsse an AT absolut auf Basis der bewilligten Projekte

55,4 Mio. €

[1] Ergebnisse Studie „Österreichs Beteiligung am europäischen Sicherheitsforschungsprogramm – Effekte für beteiligte Einrichtungen und das Innovationssystem"
* inkl. Mehrfachbeteiligungen einzelner Institutionen

Inhalt

AQUS II

Ausbildungs- und Qualitätsstandards für Sicherheitsdienstleister*innen

Entwicklung von Berufsbildern und Curricula mit Schwerpunkt möglicher Lehrberuf und Fokus auf kritischer Infrastruktur sowie Großveranstaltungen

Bis dato ist es in Österreich nicht gelungen, einheitliche Ausbildungs- und Qualitätsstandards für private Sicherheitsdienstleister*innen zu implementieren. Die Schaffung von verbindlichen Qualitätsstandards, die Entwicklung eines Berufsbildes sowie eines entsprechenden Lehrberufes sind im Regierungsprogramm 2020-2024 als Maßnahme für den Bereich Innere Sicherheit enthalten.

Aufbauend auf den Ergebnissen des Vorprojekts „AQUS (I)“ aus 2017/18 wurden in AQUS II ab Oktober 2020 Faktoren erforscht, die die Umsetzung einer verpflichtenden Aus- und Weiterbildung und entsprechender Berufsbilder hemmen oder fördern. Darüber hinaus wurden mit den relevanten Stakeholdern abgestimmte Curricula entwickelt.

Im Rahmen einer System- und Akteursanalyse wurden aktuell fördernde und hemmende Faktoren auf Makro-, Meso- und Mikroebene in Österreich identifiziert, bestehende internationale Berufsbilder und Curricula analysiert sowie relevante künftige Bedrohungslagen erhoben.

In dem mehrstufigen Prozess wurden zunächst die Anforderungen von Stakeholdern erhoben; außerdem fanden Veranstaltungen und Textdiskussionen in unterschiedlichen Formaten statt (COVID19-bedingt teilweise online mit Hilfe des Tools eComitee). Rund 100 Personen brachten hier ihre Erfahrungen und Expertise ein. Flankierend dazu wurden zwei Online-Umfragen bei Unternehmen bzw. Organisationen der kritischen Infrastruktur durchgeführt und ausgewertet.

Curricula-Entwicklung für drei Ausbildungs-Lücken

Im Rahmen des Projekts wurden drei besonders relevante Ausbildungs-„Lücken“ identifiziert.

- Curriculum A beschreibt mögliche Inhalte für eine „2-tägige Schulung für (gelegentlich) Beschäftigte bei Veranstaltungen“ im Umfang von 16 Lehreinheiten mit Schwerpunkt auf E-Learning.
- Curriculum B listet Struktur und Inhalte eines möglichen „Lehrgangs für Sicherheitspersonal in der kritischen Infrastruktur“ auf. Hier diente die in Deutschland etablierte „Geprüfte Schutz- und Sicherheitskraft (IHK)“ als Orientierungsgrundlage. Dafür sind 264 Lehreinheiten vorgesehen.
- Curriculum C umfasst Inputs für einen „Lehrberuf Sicherheit“ (Arbeitstitel) –mit einem breit aufgestellten Berufsbild. Auch hier diente die Situation aus Deutschland als Vorbild, wo neben Bewachungsunternehmen etwa auch Kommunen oder Kritische-Infrastruktur-Einrichtungen ausbilden.

Die vorgeschlagenen Ausbildungsangebote sind nicht aufeinander aufbauend, da sie unterschiedliche Zielgruppen und Bedarfe adressieren.

In der Folge wird eine schemenhafte Einordnung in den Stufen des Nationalen Qualifikationsrahmens dargestellt. Dies dient der Illustration und soll einer Zuordnung durch NQR-Servicestellen im Rahmen des vorgesehenen Verfahrens keinesfalls vorgreifen (dazu müssten Bildungsanbieterinnen und -anbieter ein Ersuchen zur Einordnung eines konkreten Bildungsangebots stellen). Für Lehrberufe ist eine Zuordnung im Verbund auf Stufe IV erfolgt.

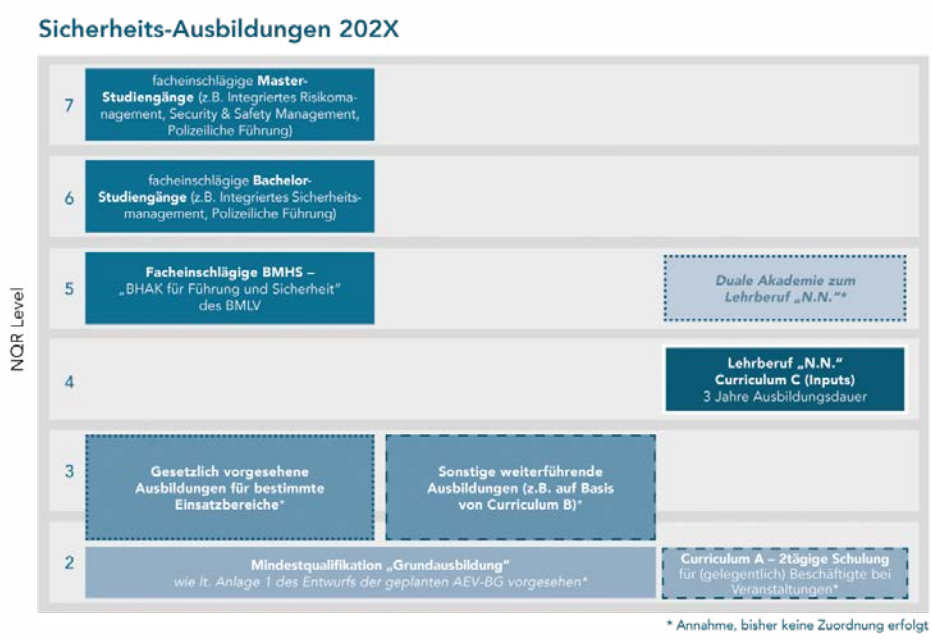


Abb.: Plan für Sicherheits-Ausbildungen

Als Begleitmaßnahme wird u.a. eine Informationskampagne durch Branchenvertretungen bzw. Ausbildungsbetriebe empfohlen.

Projektabschluss und finale Bemerkung

Das Projekt wurde im Oktober 2021 mit einer Fachkonferenz an der FH Campus Wien und der Präsentation eines Kurzberichts inhaltlich abgeschlossen. Die Ergebnisse des Projekts wurden von Projektleiterin Claudia Körmer bei der KIRAS Konferenz 2022 präsentiert.

Ausdrücklich festzuhalten ist, dass die Ergebnisse keinen durchgehenden fachlichen Konsens der Projekt-beteiligten hinsichtlich der Inhalte und der organisatorischen Umsetzung darstellen können. Sie stellen keinen Konsens der Partner*innen und weiteren Beteiligten dar und präjudizieren bzw. ersetzen somit selbstverständlich nicht deren bestehende oder künftige Meinungsbildungen, Beschlüsse, Positionierungen etc.

Projektleitung:

FH Campus Wien

Projektpartner:

- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung
- Bundesministerium für Digitalisierung und Wirtschaftsstandort
- Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
- Verband Akademischer Sicherheitsberater Österreichs
- Verband der Sicherheitsunternehmen Österreichs
- Donau-Universität Krems
- Gewerkschaft vida
- Wiener Gesundheitsverbund
- Parlamentsdirektion
- Wiener Linien
- Wirtschaftskammer Österreich

Kontakt:

FH-Prof.in Mag.a Claudia Körmer
FH Campus Wien
Favoritenstraße 226, 1100 Wien
T: +43 1 606 68 77-2164
claudia.koermer@fh-campus-wien.ac.at
www.fh-campuswien.ac.at

AIFER

Künstliche Intelligenz zur Analyse und Fusion von Erdbeobachtungs- und Internetdaten zur Entscheidungsunterstützung im Katastrophenschutz

Einleitung

Katastrophenereignisse und Großschadenslagen wie beispielsweise Hochwasser, Waldbrände, extreme Schneelagen oder Stürme stellen den Katastrophenschutz zunehmend vor große Herausforderungen in Bezug auf (1) Verfügbarkeit und Verwendung von echtzeitnaher und großflächiger Information zur Lageerfassung und -einschätzung, (2) Auswertung der Daten in naher Echtzeit und (3) Fusion von abgeleiteten Informationsebenen für intuitive, transparente und fokussierte Entscheidungsunterstützung. Das AIFER-Projekt erforscht, wie Informationen aus innovativen Datenquellen (Posts aus geo-sozialen Medien sowie Satelliten- und Drohnenbilder) mit Hilfe von KI-Forschung analysiert und fusioniert werden können. Die generierte Information trägt zur rascheren und genaueren Lageeinschätzung bei, was folglich die Gewährleistung von Schutz und Rettung von Menschen und kritischer Infrastruktur unterstützt. Die Forschungsergebnisse wurden in einem realitätsnahen Anwendungsfall in der Praxis erprobt: Die großflächige Katastrophenübung beschäftigte etwa 900 Einsatzkräfte. Sie war rund um ein Jahrhunderthochwasserereignis konzipiert und adressierte vier Einsatzabschnitte, nämlich einen Gebäudeeinsturz, überflutete Gebäude, die Entgleisung eines Gefahrengutzuges sowie treibende Personen in einem Fließgewässer. Die Koordination der Übung erfolgte durch einen professionellen Einsatzstab, der digitale Echtzeitinformation für die Lagebewältigung nutzte. Die Ergebnisse der Übung zeigen, dass digitale Datenquellen für die Lagebeurteilung und Stabsarbeit einen entscheidenden Mehrwert liefern können, sowohl in Bezug auf rasche Situationseinschätzung als auch auf effiziente Ressourcen- und Einsatzplanung.

Digitale Information im Realeinsatz

Die Verfügbarkeit von digitalen Datenbeständen hat im vergangenen Jahrzehnt drastisch zugenommen. Posts in geo-sozialen Medien sowie Fernerkundungsdaten von Satelliten und Drohnen können einen entscheidenden Mehrwert in der schnellen Lagebeurteilung und -bewältigung liefern. Für die Analyse dieser digitalen Datenbestände kommen durchwegs KI-Methoden zum Einsatz, bspw. in der semantischen Analyse von Social-Media-Text, der Relevanzklassifizierung von Posts, der Gebäude- und Fahrzeugdetektion in Bilddaten sowie der Abgrenzung von Überflutungsflächen.

Abbildung 1 zeigt aus Twitter und Facebook extrahierte Posts mit Geolokation sowie die dazugehörige Hotspot-Karte, die aktuelle räumliche Häufungen von Social-Media-Posts offenbart. Über die Hotspots hinaus werden auch Einzelposts inkl. Text, Bilder und Videos dargestellt.

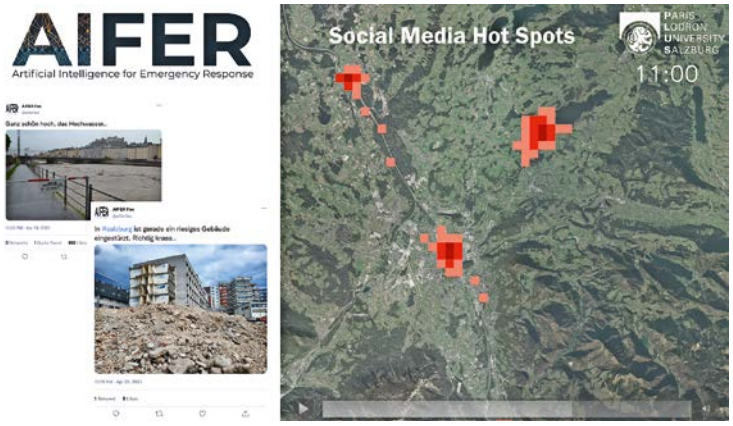


Abb. 1: Social-Media-Posts und -Hotspots

Abb. 2: Satelliten- und Drohnenbilder

Schlussfolgerungen

Abschließend kann festgestellt werden, dass der Einsatz digitaler Datenbestände wie Social-Media-Posts und Fernerkundungsbilddaten sowie KI-Analysen eine wichtige Erweiterung für Lagebeurteilung und Einsatzunterstützung bieten.

Neben der Bereitstellung der Information sowie deren Nutzung in der Stabsarbeit wurde auch deren Nützlichkeit evaluiert. Die Rückmeldung der Stabsmitarbeiterinnen und -mitarbeiter war durchwegs sehr positiv, wobei die Nutzung von neuartiger digitaler Information proaktiv in den Katastrophenmanagementprozess eingebunden werden muss, um auch im Ernstfall darauf zurückgreifen zu können. Dies bedarf einerseits einer Schulung der Stabsmitarbeiterinnen und -mitarbeiter, andererseits einer Weiterentwicklung der Informationsebenen in Bezug auf Relevanz, Genauigkeit und Verlässlichkeit.

Ein Nachbericht der Übung kann auf der Website des Salzburger Landesmedienzentrums nachgesehen werden: https://service.salzburg.gv.at/lkorrj/detail?nachrid=68452

Darüber hinaus wurde ein Ausbildungsfilm erstellt, um das Katastrophenmanagement künftig mit neuesten wissenschaftlichen Erkenntnissen zu verbessern: https://www.youtube.com/watch?v=F5JXu7Du42A

Projektleitung:

Paris-Lodron-Universität Salzburg

Projektpartner:

- Institut für empirische Sozialforschung GmbH
- Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH
- Österreichisches Rotes Kreuz – Landesverband Salzburg
- Spatial Services GmbH
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)
- Universität Kassel
- Bundesanstalt Technisches Hilfswerk (THW)
- Bayerisches Rotes Kreuz
- Disy Informationssysteme GmbH

Kontakt:

Assoz.-Prof. Dr. Bernd Resch
Universität Salzburg, Fachbereich Geoinformatik – Z_GIS
Schillerstraße 30
5020 Salzburg
Tel: +43 662 8044 7551
E-mail: bernd.resch@sbg.ac.at
zgis.at

B.PREPARED

Notfallplanungs- und Entscheidungshilfesystem für Unfälle mit Gefahrstoffen

Motivation und Zielsetzung

Das Bewältigen eines Unfalls mit CBRN-Gefahrstoffen bzw. toxischen Industriematerialien stellt eine enorme Herausforderung für alle Beteiligten dar. B.PREPARED hat sich zum Ziel gesetzt, ein Notfallplanungs- und Entscheidungshilfesystem für Unfälle mit Gefahrstoffen zu konzipieren, welches durch vorbereitende Datenerhebung, laufende Aktualisierung des Bedrohungsbildes, geregelten Informationsaustausch sowie über Modellrechnungen erstellte Gefährdungsprognosen dem jeweils aktuellen Informationsstand entsprechende Entscheidungsgrundlagen verfügbar macht und die Prozesse aller beteiligten Parteien medienbruchfrei unterstützt.

Workshops

Zum Erheben des Ist-Standes im Hinblick auf verwendete Prozesse und Werkzeuge sowie von konkreten Anforderungen an das zu konzipierende Notfallplanungs- und Entscheidungshilfesystem wurden Stakeholder-Workshops veranstaltet.

Im Rahmen der Workshops wurden die nach Stand der Technik und Wissenschaft verfügbaren meteorologischen Eingangsdaten und kleinräumigen Störfallmodelle vorgestellt und die Anforderungen an das Modellergebnis aus Sicht der Einsatzkräfte sowie Herausforderungen bei der Erfassung der erforderlichen Modelleingangsdaten diskutiert. In Arbeitsgruppen wurden Systemanforderungen gesammelt und mit dem Ist-Stand verglichen sowie Fragestellungen zur Notfallkommunikation besprochen.

Projektarbeit und bisherige Ergebnisse

Mit aktuellem Stand (Juni 2023) befindet sich das Projekt in der Realisierungsphase des Laborprototyps des Notfallplanungs- und Entscheidungshilfesystems und der Planung zu dessen Evaluierung.

Als Arbeitsgrundlage wurden Szenarien und Daten gesammelt, die auf Notfallplänen und Unfalldaten sowie vorhandenen Datensätzen von Behörden basieren, und eine Analyse möglicher Anwendungsfälle im Rahmen von Literatur- und Fallstudien wurde durchgeführt. In Zusammenarbeit mit Stakeholdern sowie Projektpartnerinnen und Projektpartnern wurden daraus Referenzszenarien entwickelt. Ein Prozess für die Lagebeurteilung und Folgenabschätzung von Unfällen mit Gefahrstoffen wurde definiert, welcher die benötigten Daten und Kommunikationswege beschreibt. Die Notwendigkeit der Integration bestehender Prozesse und Strukturen sowie die Fähigkeiten der Beteiligten zur Datensammlung für Modellrechnungen werden dabei berücksichtigt.

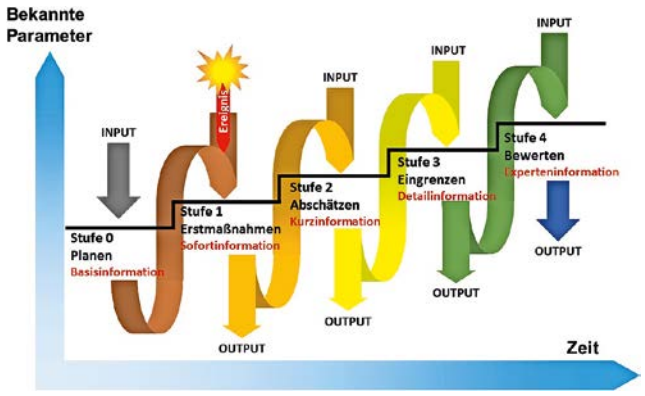


Abb.: Mehrstufiger Prozess in Abhängigkeit von Zeit und verfügbaren Informationen

Remote abrufbare Services zur Simulation von lokalen oder regional relevanten Störfallereignissen mit Freisetzung gefährlicher Gase wurden entwickelt und in einer Testumgebung erprobt. Die Testläufe für die gewählten Unfallszenarien Bahnhof Graz und Chemiepark Linz haben gezeigt, dass Berechnungen mit einem modernen Ausbreitungsmodell unter Berücksichtigung der Strömungsbeeinflussung durch Gelände sowie durch Gebäude grundsätzlich mit einer für die Lagebeurteilung geeigneten Antwortzeit (typischerweise 5 bis 10 Minuten) möglich sind. Die Windfeldsimulationen mit Gebäudeeinfluss müssen hierfür bereits vorbereitet in Form einer Bibliothek für alle Windrichtungen zur Verfügung stehen.
Die fachlichen und technischen Anforderungen an das Portal als Drehscheibe des Notfallplanungs- und Entscheidungshilfesystems sowie jene zur Berücksichtigung von Gender-&-Diversity-Aspekten wurden in einem im Konsortium abgestimmten Dokument festgehalten. Auf dieser Basis wurde eine erste Version des Portals umgesetzt, anhand deren über Strukturierung und Funktionalität sowie über die Gestaltung der Benutzeroberfläche diskutiert werden kann und welche unter Berücksichtigung von Rückmeldungen laufend weiterentwickelt wird. Aus Stakeholder-Interviews – mit Landeswarnzentralen, Medien, Rundfunk, Betreibern von digitalen Anzeigen im öffentlichen Raum – wurden Anforderungen und mögliche Schnittstellen im Bereich Notfallkommunikation abgeleitet.

Weiterer Projektverlauf und Ausblick

Die Anwendbarkeit und Einsatztauglichkeit der im Projekt erarbeiteten Prozesse und technischen Unterstützungswerkzeuge werden anhand von repräsentativen Szenarien gemeinsam mit den Bedarfsträgerinnen und Bedarfsträgern in Form zweier Tabletop Exercises – Transportunfall und betrieblicher Störfall, teilweise mit Unterstützung von Virtual Reality Training (XVR) – evaluiert. Die daraus gewonnenen Erkenntnisse werden bei der Fertigstellung des Portallösungsprototyps und der operationellen Services für die Prognoserechnung berücksichtigt. Die Mitglieder des Konsortiums werden die Nachnutzung der gewonnenen Erkenntnisse und der erstellten Lösungen weiter erörtern. Ideen für darauf aufbauende Projekteinreichungen sind zum Zeitpunkt der Erstellung dieses Berichts bereits in intensiver Diskussion, die Verwendung von Teilen der im Projekt entwickelten Portallösung für ein noch 2023 startendes Projekt mit EU-Förderung ist angedacht.

Projektleitung:

Joanneum Research

Projektpartner:

- Berufsfeuerwehr Graz
- Bundeshauptstadt Wien, MA 68 Feuerwehr und Katastrophenschutz – Berufsfeuerwehr Wien
- Bundesministerium für Landesverteidigung
- Chemiepark Linz Betriebsfeuerwehr GmbH
- Disaster Competence Network Austria – Kompetenznetzwerk für Katastrophenprävention
- HEXAGON
- IRIS – Industrial Risk and Safety Solutions e.U.
- Landeshauptstadt Graz, Magistratsdirektion, Sicherheitsmanagement und Bevölkerungsschutz
- Landesfeuerwehrverband Oberösterreich
- GeoSphere Austria

Kontakt:

Harald Lernbeiß, BSc.
JOANNEUM RESEARCH
Forschungsgesellschaft mbH
Forschungsgruppe Cyber Security and Defence
Steyrergasse 17
8010 Graz
Tel: +43 316 876 1120
E-Mail: harald.lernbeiss@joanneum.at
www.joanneum.at/digital

CATCH-IN

Technologien und Konzepte zur Ortung und Verfolgung von Interferenzquellen

Die Abhängigkeit sicherheitskritischer Infrastruktur oder zukünftiger Schlüsseltechnologien von globalen Satellitennavigationssystemen (GNSS) als Informationsquelle für Zeit und Ort wird in Zukunft weiter zunehmen. Heute schon stützen sich zahlreiche Dienste in Bereichen wie Finanzmarkt, Telekomnetze, Stromnetze, Straßennetze und Flugverkehr auf Zeit- und/oder Positionslösungen von GNSS. So werden beispielsweise auf den österreichischen Autobahnen und Schnellstraßen GNSS-basierte Anwendungen zunehmend für die Digitalisierung der Infrastruktur genutzt und Dienste zum kooperativen und vernetzten Fahren, wie beispielsweise die Übermittlung von Baustelleninformationen an Verkehrsteilnehmerinnen und -teilnehmer, immer weiter ausgebaut. Im Bereich der Flugsicherung gibt es europaweite Pläne zur Reduktion der Infrastrukturkosten und der Treibhausgasemissionen, wodurch es zu einem verstärkten Einsatz von GNSS in unterschiedlichen Flugphasen kommt. Einen Überblick über Bereiche des täglichen Lebens, die GNSS Dienste bereits heute intensiv nutzen, bietet nebenstehende Abbildung.

Störungen im GNSS-Empfang können folglich erheblichen Schaden anrichten, sowohl sicherheitstechnisch als auch wirtschaftlich. Im Falle der Dienste der österreichischen Autobahnen würde dies bedeuten, dass ortsbasierte Dienste, die in der Automatisierung des Straßenverkehrs und in der Digitalisierung im Infrastrukturbetrieb eine wichtige Rolle spielen, verfälscht sind oder überhaupt nicht zur Verfügung stehen. In der Luftfahrt und Flugsicherung können GNSS-Störungen speziell im Anflugbereich zu Sicherheitsrisiken und einem erhöhten Stresslevel bei Fluglotsen führen. Durch den zunehmenden Einsatz von GNSS wird sich dieses Problem in Zukunft verstärken.

Das Projekt CATCH IN zielt auf Innovationen zum Schutz sicherheitskritischer Anwendungen ab, die auf den Empfang von Radiowellen angewiesen sind und GNSS nützen. Im Kontext eines bundesweiten Monitoringsystems für Frequenzstörungen wird ein hybrides Monitoringsystem erforscht, das unterschiedliche Sensortechnologien kombiniert, die unter Verwendung von Schnittstellen gemeinsam genutzt werden können. Dieses Monitoringsystem soll Möglichkeiten zur Echtzeit-Identifizierung und -Lokalisierung einer Störquelle bieten. Teil dieses Systems ist einerseits ein innovativer Direction-of-Arrival (DoA)-Ansatz unter Nutzung einer rotierenden Antenne, der eine hochgenaue Lokalisierung ermöglicht. Andererseits wird auch ein Time-Difference of Arrival (TDoA)-Ansatz untersucht und umgesetzt, der unter Verwendung von Low-cost-SDR-basierten Sensoren eine Lokalisierung von Interferenzquellen ermöglicht. Dieser TDoA-Ansatz soll ein Enabler für zukünftige große Monitoringnetze wie auch für den mobilen Einsatz sein.
In Messkampagnen wird auch die Sensitivität von GNSS-Empfängern auf Störungen untersucht, ebenso wie die Kritikalität von GNSS-Störungen für die Flugsicherung und auf Flugzeuge im Start- und Landebereich.

Auf Basis dieser Ergebnisse werden Anforderungen für zukünftige Monitoringsysteme hergleitet. Begleitend werden sozialwissenschaftliche Untersuchungen durchgeführt, um das Beanspruchungserleben von Fluglotsen durch GNSS-Störungen analysieren zu können, und damit einhergehende Aspekte auf die Flugsicherheit. Als Modellobjekt dient hier ein Flughafen in Österreich. Ein Monitoringkonzept für die Flugsicherung im Start- und Landebereich wird für diesen Flughafen ausgearbeitet. Basierend auf diesem Konzept werden auch stationäre Sensorknoten installiert und längerfristige Messungen – zumindest 2 Monate – durchgeführt.

Das Gesamtziel des Projekts ist eine deutliche Verbesserung des Wissensstandes über das Auftreten und die Auswirklungen von Interferenz, Jamming und Spoofing sowie gleichzeitig die Konzeptionierung, Umsetzung und Untersuchung von geeigneten Gegenmaßnahmen. Somit trägt das Vorhaben zu einer Steigerung der Widerstandsfähigkeit kritischer Infrastruktur und zur Unterstützung von Innovationen bei.

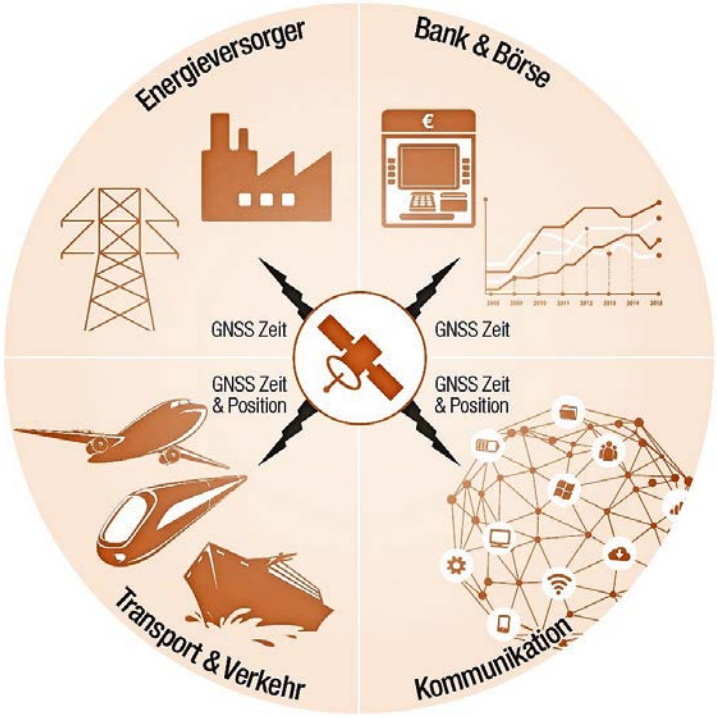


Abb.: Bereiche des täglichen Lebens, die auf robuste GNSS-Orts- und/oder -Zeitinformationen angewiesen sind

Projektleitung:

JOANNEUM RESEARCH Forschungsgesellschaft mbH, DIGITAL

Projektpartner:

- ASFINAG Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft
- Austro Control Österreichische Gesellschaft für Zivilluftfahrt mbH
- IGASPIN GmbH
- Institut Luftfahrt, FH JOANNEUM

Kontakt:

Dr. Susanne Schweitzer
JOANNEUM RESEARCH Forschungsgesellschaft mbH
DIGITAL – Institut für Digitale Technologien
Steyrergasse 17, 8010 Graz, Austria
Tel: +43 316 876 5317
E-Mail: susanne.schweitzer@joanneum.at
www.joanneum.at/digital

CAVE

Community Engagement und Vulnerabilitäten in der Bewältigung von Epidemien

Das KIRAS-Projekt CAVE (Community Engagement und Vulnerabilitäten in der Bewältigung von Epidemien) ist ein transdisziplinäres Forschungsprojekt zur angewandten Pandemieforschung in Österreich. Sozialwissenschaften (Medizinanthropologie und Psychologie), Geowissenschaft (Geoinformatik), Politik, Vertreterinnen und Vertreter von sozialen Hilfsorganisationen und technische Partner bereiten gesellschaftliche Erkenntnisse während der Covid-19-Pandemie auf, um daraus inklusive Partizipationsmodelle sowie kommunikationstechnologische Lösungen für künftige epidemiologische Gefährdungen zu entwickeln. Die Laufzeit beträgt insgesamt 2 Jahre, von Oktober 2021 bis September 2023 (https://www.meduniwien.ac.at/web/forschung/projekte/cave/cave/).
Das Projekt CAVE hat zum Ziel, vulnerable Gruppen in Österreich, die durch Epidemien besonders gefährdet sind, rasch und genau zu definieren und zu erfassen, um diese wirksam in die Gestaltung und Umsetzung von Gesundheitsmaßnahmen einzubinden und mit neuen Kommunikationstechnologien besser zu erreichen. Die sozial- und geowissenschaftliche Forschung setzt ihre Schwerpunkte auf eine Bestimmung und Verortung von vulnerablen Gruppen sowie auf die Erhebung und Analyse von Erfahrungen und Bedürfnissen dieser Gruppen hinsichtlich Erreichbarkeit und Kommunikation während der Covid-19-Pandemie. Der sozialwissenschaftliche Ansatz orientiert sich am Konzept des „Community Engagement“, welches die größtmögliche Einbindung und aktive Beteiligung von vulnerablen Personen sowie deren Betreuerinnen und Betreuern ermöglichen soll (Kutalek et al 2023).

Die konkreten Ziele des Projekts CAVE bestehen in

1. der Entwicklung spezifischer und praktikabler Modelle zur Anwendung des Community- Engagement-Konzepts,
2. einer exakten und operationellen Definition von Vulnerabilität, die partizipative Prozesse berücksichtigt,
3. der Einbindung dieser Erkenntnisse in die Entwicklung von Kommunikationslösungen, um vulnerable Gruppen effektiver kontaktieren, informieren und einbinden zu können.

Grundlage aller Überlegungen und Modelle ist der in den UNICEF Minimum Standards für Community Engagement (2020) formulierte Ansatz, wonach durch vermehrte Beteiligung von Communities deren Verständnis und Akzeptanz für Interventionen gesteigert wird.
In der ersten Mapping-Phase wurden zuerst gängige Vulnerabilitätskonzepte und partizipative Modelle im Management von Epidemien und anderen Public-Health-Krisen analysiert. Im Rahmen eines qualitativen Forschungsdesigns wurden sodann auf diesen Ergebnissen aufbauend mit Mitarbeiterinnen und Mit-

arbeitern, Klientinnen und Klienten von Sozial- und Pflegeeinrichtungen sowie Expertinnen und Experten von zivilgesellschaftlichen Sozialorganisationen qualitative Interviews geführt. Hier lag der Schwerpunkt auf Fragen zu sozialer Vulnerabilität sowie zur Verständlichkeit und Umsetzbarkeit der öffentlichen Risikokommunikation und der Pandemie-Maßnahmen (Plangger et al. 2023, Wojczewski et al. 2023).
In der zweiten Phase wurden aus den Forschungsergebnissen ein Community-Engagement- und ein Vulnerabilitäts-Modell entwickelt (das CAVE-Modell). Unsere Technik-Partner erarbeiteten die Grundlage für eine Vulnerabilitäts-Landkarte von Österreich, welche lokale Schwerpunktsetzungen ermöglichen soll; die Kommunikationslösungen ermöglichen die aktive Teilhabe und Erreichbarkeit von vulnerablen Gruppen. In der dritten Phase, die auch eine Testphase ist, wird das CAVE-Modell für ein partizipatives Krisenmanagement von unseren Praxispartnern in mehreren Sozial- und Pflegeeinrichtungen auf seine Umsetzbarkeit geprüft.

Die vorläufigen Erkenntnisse (Stand Juni 2023) des Projekts lassen sich wie folgt zusammenfassen:

- Der während der Covid-19-Pandemie verwendete Vulnerabilitätsbegriff ist unzureichend, um vulnerable Gruppen in ihrer Gesamtheit und Diversität zu erfassen, und sollte vor allem um die Komponente „soziale Vulnerabilität“, aber auch um psychisch und kognitiv beeinträchtigte Personengruppen erweitert werden.
- Community Engagement, d. h. die Einbindung vulnerabler Gruppen in die Gestaltung und Umsetzung von Pandemie-Maßnahmen, ist als langfristiger Prozess zu verstehen und bedingt den Aufbau permanenter Kommunikationsstrukturen bereits vor einer Gesundheitskrise, die sowohl innerhalb von Betreuungseinrichtungen als auch zwischen diesen Einrichtungen und den Gesundheitsbehörden etabliert werden müssen.
- Kommunikationsstrukturen, die ein funktionierendes Community Engagement ermöglichen, sollen auf flachen Hierarchien innerhalb von Betreuungseinrichtungen und mit den Gesundheitsbehörden aufbauen. Je hierarchischer Kommunikationsstrukturen gestaltet sind, desto größer sind die Hindernisse für die Partizipation vulnerabler Gruppen.
- Die Möglichkeiten der Themenfindung für Community-Engagement-Prozesse sind für viele vulnerable Gruppen eingeschränkt und müssen in der Vorbereitungsphase mit entsprechenden Partizipationstechniken ausgelotet werden.
- Die Datenlage zur Verortung und Erreichbarkeit vulnerabler Gruppen in Österreich ist stark eingeschränkt und verlangt nach einer Neugestaltung der Erhebungsgrundlage unter Einbeziehung der maßgeblichen Stakeholder (Gemeinden, Gesundheitsbehörden, Betreuungseinrichtungen, Forschung und Datenschutz).

Projektleitung:

Medizinische Universität Wien

Projektpartner:

- Universität Innsbruck
- Paris Lodron Universität Salzburg
- Disaster Competence Network Austria
- Österreichisches Rotes Kreuz
- Lebenshilfe Tirol
- Spatial Services
- Safe Reach
- Bundesministerium für Landesverteidigung
- Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz

Kontakt:

Ap.Prof. Priv.-Doz. Mag. Dr.
Ruth Kutalek
Medizinische Universität Wien
Zentrum für Public Health
Kinderspitalgasse 15/1. Stock
1090 Wien
Tel: +43 1 40160 34607
E-Mail: ruth.kutalek@meduni-wien.ac.at
www.meduniwien.ac.at/hp/sozialmedizin/

CIvolunteer

Critical Infrastructures Powered by Volunteers

Freiwilliges Engagement als Grundpfeiler kritischer Infrastrukturen

Freiwilliges Engagement von Bürgerinnen und Bürgern ist ein unverzichtbarer, tragender Grundpfeiler kritischer Infrastrukturen (KRITIS) wie Katastrophenschutz, Rettungsdienst, Gesundheits- und Sozialwesen sowie Lebensmittelversorgung. Mehr als 46 % der Österreicherinnen und Österreicher sind freiwillig tätig, doppelt so viel wie im EU-Schnitt [1] [2], mit einem wöchentlichen Arbeitspensum von 14,7 Mio. Stunden[3] – davon mehr als 5,8 Mio. für KRITIS (z. B. Einsätze bei Hochwasser, Ernten, Krisenhotlines, Impfstraßen und im Pflegebereich) [4] [5] [6] [7].

KRITIS, die von freiwilligem Engagement abhängen, sind für ganz Österreich von fundamentaler Bedeutung. Eine mangelnde Tragfähigkeit des Freiwilligensektors durch

- einen Rückgang freiwilligen Engagements,
- eine Überlastung aufgrund übermäßiger Nachfrage oder gar
- einen Ausfall in Krisenzeiten, wenn Freiwillige selbst zu Hilfebedürftigen werden,

würde nicht nur die Versorgungsqualität in Nicht-Krisenzeiten gefährden, sondern vor allem auch im Krisenfall eine Aktivierung und Koordination der „besten Kräfte“ nicht mehr gewährleisten.

---

1 EU-Generaldirektion Bildung & Kultur (EAC): Freiwilligentätigkeit in der EU, https://ec.europa.eu/citizenship/pdf/executive_summary_volunteering_de.pdf [Zugriff: 16.06.2023]

2 Kals, E., Freund, S., Enders, B., and Schütt, S. C.: Stärkung des Ehrenamts im Katastrophenschutz, NRW, Katholische Universität Eichstätt-Ingolstadt, 2020, https://www.im.nrw/system/files/media/document/file/20-10-27%20KU%20Abschlussbericht%20gesamt_final.pdf [Zugriff: 16.06.2023]

3 Feistritzer, G.: Quantitative und qualitative Entwicklung des freiwilligen Engagements in Österreich. In BMASGK (Ed.), Bericht zum freiwilligen Engagement in Österreich. Freiwilligenbericht 2019, Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz, 2019

4 Trautwein, S., Liberatore, F., Lindenmeier, J., and von Schnurbein, G.: Satisfaction With Informal Volunteering During the COVID-19 Crisis: An Empirical Study Considering a Swiss Online Volunteering Platform. Nonprofit and Voluntary Sector Quarterly, 49(6), 2020, https://doi.org/10.1177/0899764020964595

5 Simsa, R., Rameder, P., Aghamanoukjan, A., and Totter, M.: Spontaneous Volunteering in Social Crises: Self-Organization and Coordination. Nonprofit and Voluntary Sector Quarterly, 48(2_suppl), 2019, https://doi.org/10.1177/0899764018785472

6 Meyer, M., and Simsa, R.: Organizing the Unexpected: How Civil Society Organizations Dealt with the Refugee Crisis. VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations, 29(6), 2018, https://doi.org/10.1007/s11266-018-00050-y

7 Simsa, R.: Leaving Emergency Management in the Refugee Crisis to Civil Society? The Case of Austria. Journal of Applied Security Research, 12(1), 2017, https://doi.org/10.1080/19361610.2017.1228026

Die Tragfähigkeit des Freiwilligensektors ist allerdings durch den demografischen Wandel, insbesondere aber auch durch den tiefgreifenden gesellschaftlichen Struktur- und Motivwandel[4] im Sinne einer Individualisierung und Pluralisierung der Gesellschaft massiv gefährdet.

CIvolunteer als digitale Plattform für freiwilliges Engagement

Das Projekt CIvolunteer (Critical Infrastructures Powered by Volunteers) trägt diesen zentralen Herausforderungen Rechnung, indem eine digitale Plattform zur zielgesteuerten und kompetenzbasierten Vernetzung und Bündelung von freiwilligem Engagement über NPO-Grenzen hinweg geschaffen werden soll, sodass Ziele und Kompetenzen von Freiwilligen mit den Tätigkeitserfordernissen zur Stärkung von KRITIS synergetisch abgestimmt werden können (siehe Abbidlung). Eine derartige Professionalisierung freiwilligen Engagements durch eine adäquate digitale Transformation schafft die Basis, um die Tragfähigkeit des Freiwilligensektors auch zukünftig sicherzustellen und so eine nachhaltige und umfassende Stärkung freiwilligenabhängiger KRITIS zu gewährleisten.

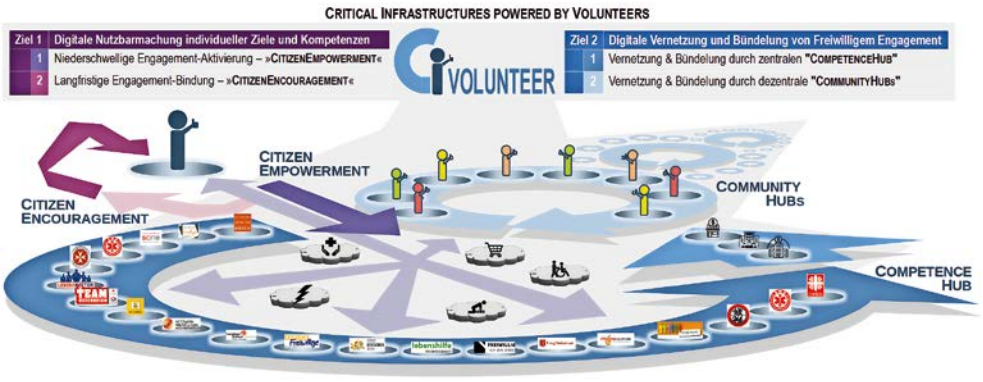


Abb.: Forschungsziele von CIvolunteer

Als zentrales Ergebnis werden erste zentrale, praxisnahe Showcases prototypisch in einer webbasierten mobilen Plattform umgesetzt, komplettiert durch die Erforschung der konzeptionellen Voraussetzungen und technischen Rahmenbedingungen sowie ein entsprechendes Geschäftsmodell zu deren Nutzbarmachung für freiwilligenabhängige KRITIS. Der methodische Ansatz folgt dem Human Centered Design Approach, indem das Projektergebnis unter Einbeziehung der Endbenutzerinnen und Endbenutzer kontinuierlich konkretisiert wird, wobei Nachhaltigkeit und adäquate Evaluierung in Kooperation mit dem Bedarfsträger und mit über LoIs assoziierten Unternehmen und NPOs aus unterschiedlichen KRITIS-Bereichen mittels Benutzerstudien sichergestellt werden. Das Konsortium vereint ein breites Spektrum interdisziplinärer Kompetenzen aus Wirtschaft und Wissenschaft mit anwendungsnahem Wissen von Bedarfsträgern und NPOs, im Besonderen aber auch von Bürgerinnen, Bürgern und Communities aus dem informellen Freiwilligensektor, die als Bedürfnisträgerinnen und Bedürfnisträger sowie Ideen-/Lösungsbringerinnen und -bringer fungieren.

Projektleitung:

Johannes Kepler Universität

Projektpartner:

- Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
- doloops accessible web technologies GmbH
- X-Net Services GmbH
- FH OÖ Forschungs und Entwicklungs GmbH
- Universität für künstlerische und industrielle Gestaltung Linz , Institut für Medien
- Wirtschaftsuniversität Wien Kompetenzzentrum für Nonprofit Organisationen und Social Entrepreneurship

Kontakt:

a.Univ.-Prof.in DIin Dr.in Birgit PRÖLL
Johannes Kepler Universität Linz (JKU)
Altenbergerstraße 69
4040 Linz
Tel: +43 664 60 2468 770
E-Mail: birgit.proell@jku.at
www.jku.at/en/institute-for-application-oriented-knowledge-processing/

CONTAIN

Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten

In Österreich und Deutschland nimmt die Bedrohung durch Cyberangriffe stetig zu. In der Vergangenheit haben bereits verschiedene Cyber-Vorfälle die Sicherheit der Zivilgesellschaft in beiden Ländern ernsthaft gefährdet. Solche Angriffe haben das Potenzial, nicht nur Unternehmen, sondern auch ganze Lieferketten nachhaltig zu beeinträchtigen, und deren Wiederherstellung gestaltet sich oft als äußerst schwierig. Die Auswirkungen solcher Ereignisse können gravierende Konsequenzen für Privatpersonen, Unternehmen und Regierungsorganisationen haben. Aus diesem Grund haben sowohl Deutschland als auch Österreich in den vergangenen Jahren erhebliche Investitionen in die IT-Sicherheit von Unternehmen getätigt, insbesondere im Bereich kritischer Infrastrukturen. Dabei wurden auch Bestimmungen der NIS-Richtlinie der Europäischen Union zur Anwendung gebracht.

Um auf diese Herausforderungen angemessen zu reagieren, ist es nun von großer Bedeutung, das Bewusstsein für die Bewältigung von Cyber-Vorfällen zu schärfen und die erforderlichen Fähigkeiten aufzubauen. Ziel ist es, im Falle einer Bedrohung die Verfügbarkeit von Diensten und kritischen Infrastrukturen so schnell wie möglich wiederherzustellen.

In diesem Zusammenhang wurde das Projekt **CONTAIN** ins Leben gerufen. Das Hauptziel von **CONTAIN** besteht darin, das **Bewusstsein für den Umgang mit Vorfällen im Bereich der Cybersicherheit zu erhöhen und entsprechende Referenzprozesse zu definieren**. Dabei konzentriert sich das Projekt auf drei Hauptaspekte: Erstens sollen die Auswirkungen von Cyberangriffen minimiert werden, zweitens strebt man an, sowohl die Anzahl als auch die Kritikalität erfolgreicher Cyberangriffe zu verringern, und drittens möchte man die Effizienz bei der Aufklärung von solchen Angriffen steigern. **CONTAIN** legt dabei besonderen Wert auf die Entwicklung und Umsetzung von Prozessen und Verfahren, die erforderlich sind, um effektiv auf IT-Sicherheitsvorfälle zu reagieren, deren Auswirkungen einzudämmen, Schwachstellen zu beheben sowie die Robustheit und Souveränität der Systeme zu erhöhen.

Das Projekt **CONTAIN** hat zum Ziel, das Bewusstsein für Incident Response und die nachfolgenden Prozesse auf eine neue Stufe zu heben sowie entsprechende Referenzprozesse zu definieren. Alle gewonnenen Erkenntnisse und Informationen werden in ein Simulationsmodell integriert, um kritische Prozesse zu identifizieren sowie mögliche Ressourcen- und Kapazitätsengpässe aufzudecken. Zudem werden relevante Möglichkeiten zur Optimierung der Prozesse abgeleitet, die insbesondere für kleine und mittlere Unternehmen (KMUs) geeignet sind.

Um diese Ziele zu erreichen, plant **CONTAIN** den Einsatz von Serious Games, also Spielen mit einem ernsthaften Zweck. Mithilfe dieser Spiele sollen die Verhaltensweisen der Benutzerinnen und Benutzer hinterfragt und operative Entscheidungsprozesse analysiert, definiert und validiert werden. Darüber

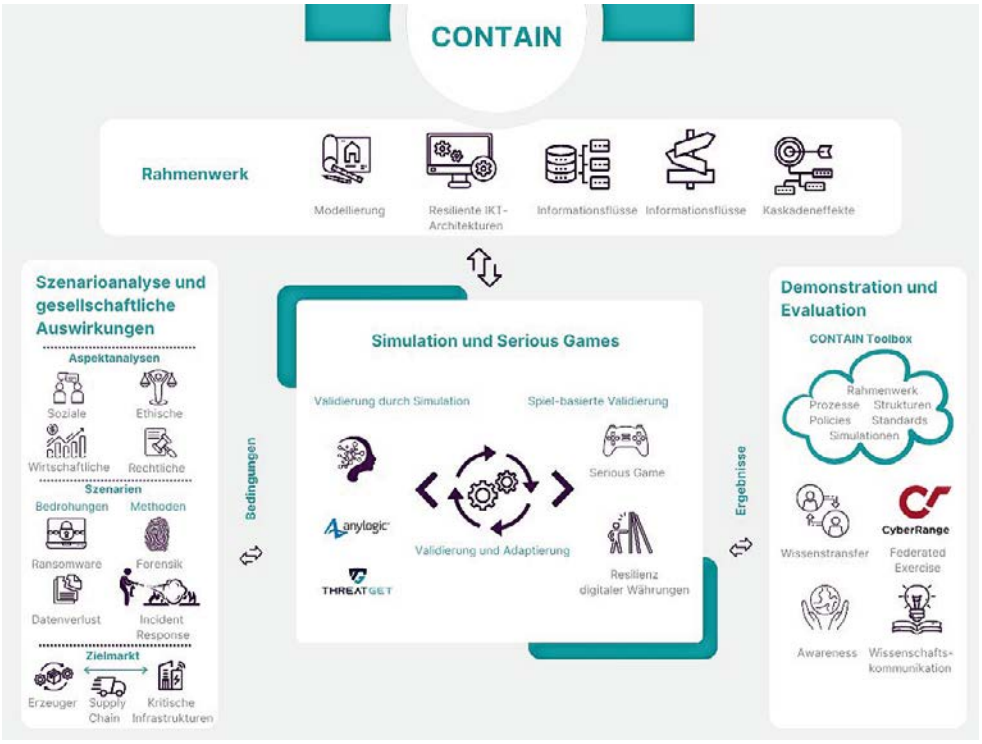


Abb.: Ein Modell, um mit Serious Games mehr Bewusstsein für Cyberbedrohungen zu schaffen

hinaus liegt ein besonderer Fokus auf der Entwicklung und Validierung eines effektiven Krisenmanagements sowie auf der Koordination der Akteure und ihrer Verantwortlichkeiten innerhalb der Lieferketten. Eine gemeinsame Forschung zwischen Österreich und Deutschland kann dazu beitragen, die erforderlichen Fähigkeiten effizient und effektiv zu etablieren und voneinander zu lernen. Die österreichische Seite profitiert insbesondere von den bereitgestellten Szenarien und Serious Games durch das deutsche Konsortium sowie von den Analysekompetenzen in Bezug auf virtuelle Währungen und Liquidität in Krisensituationen. Die deutsche Seite profitiert von der Analyse von Kaskadeneffekten sowie von Perspektiven aus dem Krisenmanagement und der Krisenkommunikation.

Beide Konsortien profitieren von gemeinsamen Aktivitäten zur Gestaltung und zur Validierung von Serious Games. Die bilaterale Zusammenarbeit soll schlussendlich helfen, nationale Vorgehensweisen in der Krisenvorsorge zu erkennen und zu reflektieren, um so zu besseren Lösungen zu kommen. Die **Anwendungsdomänen** des Projektvorhabens sind **Transport und Verkehr**, welche sowohl auf deutscher, österreichischer als auch auf europäischer Ebene als kritische Infrastruktur eingestuft sind.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Bundesministerium für Landesverteidigung
- Gartner KG
- KWIZDA HOLDING GMBH
- Roland Spedition GmbH
- team Technology Management GmbH
- Universität für Bodenkultur Wien
- Universität Wien
- VICESSE Research GmbH

Kontakt:

Gregor Langner, MSc.
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 664 883 90 672
E-Mail: gregor.langner@ait.ac.at
www.ait.ac.at

CyberMonoLog

Erarbeitung von Best-Practice-Guidelines für Cyber-Security-Monitoring und Logging basierend auf den bekannten Angriffstechniken lt. MITRE ATT&CK

Während jahrzehntelang bei der Cyber-Security der Fokus auf Prävention und Perimeter-Sicherheit lag, hat sich die Ausrichtung in den letzten Jahren in Richtung aktiver Reaktion gewandelt. Es gilt als allgemein anerkannt, dass eine komplexe Infrastruktur auf Dauer nicht erfolgreich vor Angriffen geschützt werden kann. Daher ist es wichtig, das Zeitfenster der Angreifer – vom initialen Eindringen bis zu deren Entdeckung und dem Ergreifen von ersten Gegenmaßnahmen – auf die kürzestmögliche Zeitspanne zu reduzieren. Damit verringern sich auch die Möglichkeiten der Angreifer, schon das initiale Eindringen in ein Netz für einen erfolgreichen Angriff zu nutzen (d. h. das Erreichen der eigentlichen Ziele sicherzustellen, wie das Exfiltrieren von Daten oder das Lahmlegen einer Infrastruktur). Das Erkennen von Angriffen und die rasche Reaktion darauf sind daher essenzielle Fähigkeiten für Organisationen – nicht nur für die Großindustrie, sondern auch für kritische Infrastrukturanbieter (KI) und für den in Österreich so wichtigen KMU-Sektor. Gerade diese agieren jedoch oft unter enormem Kostendruck, was dem üblicherweise ressourcenaufwendigen Einsatz komplexer Cyber-Security-Lösungen entgegensteht. Zudem sind Betreiber wesentlicher Dienste nach dem NISG auch dazu verpflichtet, Cyber-Security-Lösungen nach dem Stand der Technik zum Einsatz zu bringen.

Ziel des Projekts war daher die Erarbeitung von Best Practices für Cyber-Security-Monitoring und Logging (CyberMonoLog), basierend auf den bekannten Angriffstechniken und unter besonderer Berücksichtigung jener, welche nicht durch allgemein angewandte Best Practices/Standards bereits effektiv unterbunden werden. Angriffstechniken, welche aus wirtschaftlicher oder technischer Sicht typischerweise reaktiv behandelt werden, müssen durch Monitoring aufgedeckt werden. Letztendlich lag dem Projekt somit ein Optimierungsproblem zugrunde: Es ist für eine Organisation unmöglich, alle bekannten Angriffstechniken mit ökonomischen Mitteln zu erkennen. Die Forschungsfrage war daher, welche Datenquellen (bzw. davon emittierte Ereignisse) mit welchen Methoden analysiert werden müssen (Ranking), um mit vorab festgelegtem Ressourceneinsatz die meisten relevanten Angriffstechniken zu erkennen.

Die Ergebnisse des Projekts sind praxisnahe Best-Practice-Guidelines zur Umsetzung einer Monitoring-Strategie für KMUs und KIs. Die Ausführungen stützen sich auf den bekannten Stand der Technik, und die Anwendbarkeit der Ergebnisse wurde durch eine Cross-Validierung mit externen Stakeholdern sowie Bedarfsträgern und Behörden und Experten von CERT.at sichergestellt. Rechtliche Aspekte (Datenschutz, arbeits-/dienstrechtliche Belange) wurden ebenso berücksichtigt.

Im Detail wurden somit im Projekt CyberMonoLog die folgenden Ziele erreicht: (1) Relevante Angriffstechniken wurden aus dem MITRE ATT&CK Framework erhoben und anhand ausgewählter Metriken (Verbreitung, Impact, Anwendbarkeit usw.) gereiht. (2) Ein Modell, welches zur Lösung des angesprochenen Optimierungsproblems geeignet ist, wurde formuliert und beispielhaft anhand einer Microsoft-365-Umgebung instanziiert, um dessen Tauglichkeit zur Bewertung von Monitoring-Lösungen in spezifischem Kontext zu beurteilen. (3) Weiters wurde ein Survey anwendbarer Standards und Empfehlungen im Bereich Logging und Monitoring (CIS Top18, ISO27001/2, BSI Grundschutz usw.) durchgeführt und Gemeinsamkeiten hinsichtlich Anforderungen an Logging- und Monitoring wurden erhoben. (4) Ein Survey unter KMUs (200 Teilnehmer) zur Feststellung wesentlicher Assets und Technologien bzw. Umgebungen im KMU-Bereich, die Monitoring und Logging bedürfen, wurde durchgeführt, um den Scope der weiteren Betrachtungen, insbesondere der Erstellung konkreter Handlungsempfehlungen, abzugrenzen. (5) Aufbauend auf den erhobenen relevanten Technologien/Assets und unter Zuhilfenahme des Optimierungsmodells wurde die erste Iteration der Umsetzungsempfehlungen in Form von Guidelines in mehreren weiteren Iterationen wesentlich verbessert, wobei detaillierte Schritt-für-Schritt-Anleitungen über Referenzen eingebunden und konkret ausformuliert wurden. (6) Mit Hilfe von „trusted partners“ wurden Feedback-Gespräche mit Branchenvertretern der Zielgruppe (KMUs und KIs) geführt. (7) Rechtliche Fragen, v. a. hinsichtlich Daten-Erhebung (Logging), Langzeitarchivierung von Logs und systematischer Verarbeitung, wurden erhoben, betrachtet und bewertet. (8) Die erarbeiteten Guidelines wurden in einer WKO-Awareness-Kampagne an deren Mitglieder im Juni 2023 großflächig verteilt.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- SBA Research gemeinnützige GmbH (gGmbH)
- Computer Emergency Response Team/NIC.at
- TU Wien (Prof. Haslinger)
- Bundesministerium für Inneres
- Bundeskanzleramt

Kontakt:

Dr. Dr. Florian Skopik
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 664 8251495
E-Mail: florian.skopik@ait.ac.at
www.ait.ac.at

defalsif-AI

Detektion von Falschinformation mittels Artificial Intelligence

Das Thema „Fake News“ und die Frage, wie wir Falschnachrichten besser erkennen können, hat in den letzten Jahren stark zugenommen. Dafür waren vor allem internationale Konflikte, Versuche zur Meinungs- und Wahlbeeinflussung, die Zunahme der Cyberkriminalität und technologische Entwicklungen verantwortlich. Ziel des Forschungsprojekts „defalsif-AI“ (Detektion von Falschinformation mittels Artificial Intelligence) war es, ein Werkzeug für die Analyse von Texten, Bildern, Videos oder Audioaufzeichnungen im Internet zu erarbeiten. Dieses soll eine Empfehlung abgeben, ob man einem bestimmten Inhalt vertrauen kann – oder nicht.

Viele Analyseverfahren

Dazu kommen eine Vielzahl an unterschiedlichen Analyseverfahren und medienforensische Werkzeuge zum Einsatz, die in einem gemeinsamen System zusammengeführt werden. Jedes einzelne dieser Analyseverfahren liefert für sich nachvollziehbare Ergebnisse, die in einer einheitlichen und verständlichen Benutzeroberfläche dargestellt werden. Zudem wird die Software aus rechts- und sozialwissenschaftlicher Perspektive beurteilt. Das Projekt wird im Rahmen des österreichischen Sicherheitsforschungs-Förderprogrammes KIRAS gefördert. In Summe waren neun Projektpartner aus unterschiedlichen Bereichen beteiligt. Das Projekt hat im Oktober 2020 begonnen und lief bis September 2022.

Politisch motivierte Desinformation

defalsif-AI adressiert im Kontext medienforensische Werkzeuge (Hybrid-Threats – Fake-News) insbesondere politisch motivierte Desinformation, welche politische sowie staatliche Institutionen unserer Demokratie – z. B. Wahlbeeinflussung – und somit letztlich das öffentliche Vertrauen in politische und staatliche Institutionen schwächt bzw. bedroht. Die inhaltlichen Forschungsschwerpunkte liegen auf audiovisueller Medienforensik, Textanalyse und deren multimodaler Fusion unter Zuhilfenahme von Methoden der künstlichen Intelligenz (KI). Ein Hauptaugenmerk liegt dabei auf der nachvollziehbaren und interpretierbaren Präsentation der Ergebnisse, um eine möglichst breite Anwender- und Anwenderinnenbasis zu erreichen und optimal zu unterstutzen.

Projektziel

Das Ziel des Projektes war, ein Proof-of-Concept-Werkzeug für die Analyse von digitalen Inhalten im Internet zu demonstrieren, das eine erste Beurteilung der Inhalte (Text, Bild, Video, Audio) auf Glaubwürdigkeit/Authentizität ermöglicht und so die Grundlagen für weitere Handlungsempfehlungen schafft. Eine umfassende Analyse und Beurteilung des medienforensischen Werkzeugs aus rechts- und sozial-

wissenschaftlicher Perspektive, die Ableitung von anwendungsorientierten, technischen und organisatorischen Maßnahmen sowie ein Verwertungsplan für den zukünftigen Betrieb rechtsstaatlich konformer Desinformationsanalyseplattformen haben das Projekt abgerundet.

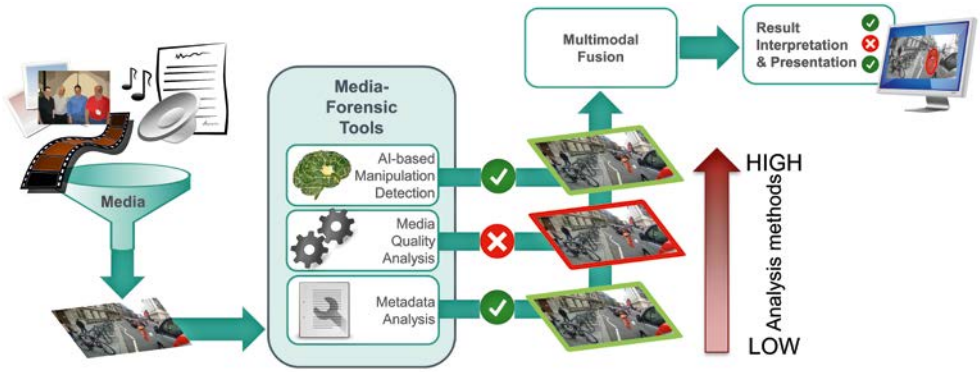


Abb.: Wie funktioniert ein medienforensisches Werkzeug

Projektleitung:

AIT Austrian Institute of Technology GmbH

Projektpartner:

- APA – Austria Presse Agentur
- Donau-Universität Krems
- EnliteAI GmbH
- Research Institute AG & Co KG
- Bundeskanzleramt Österreich
- Bundesministerium für Landesverteidigung
- Bundesministerium für Europäische und Internationale Angelegenheiten
- ORF – Österreichischer Rundfunk

Kontakt:

Martin Boyer
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4284
martin.boyer@ait.ac.at
www.ait.ac.at

DELOREAN

Die Elektromobilität im realen Praxiseinsatz bei der Polizei

Die steigende Verfügbarkeit von Elektrofahrzeugen sowie die politische Zielsetzung im Hinblick auf Klimaschutz und Energieeffizienz führen dazu, dass neben privaten Nutzerinnen und Nutzern auch die öffentliche Verwaltung und die Behörden verstärkt auf Elektromobilität setzen. Die Polizei verfügt mit über 6.000 Fahrzeugen über die größte Fahrzeugflotte in Österreich und plant eine schrittweise Integration von Elektromobilität. Hierbei müssen sehr spezifische Anforderungen erfüllt werden, um jederzeit die unmittelbare Einsatzbereitschaft und damit die Sicherheit der Bevölkerung zu gewährleisten.

Neben Herstellerangaben ist es essenziell, die tatsächliche Energienutzung und die maximale Reichweite unter bestimmten Umgebungsbedingungen zu kennen. Dafür werden Datenlogger im Fahrzeug installiert, welche nach Relevanz für das Flottenmanagement ausgewählte Daten aufzeichnen. Diese Daten zur Analyse des Realbetriebs erfassen das Fahrerverhalten, zurückgelegte Strecken und damit Topografie, Umgebungstemperaturen und Daten über die elektrischen Verbraucher. So wird es dem BMI ermöglicht, den Fahrzeugeinsatz, die Ladeinfrastruktur und die Kosten zu justieren, was letztlich einen effizienten Einsatz von Steuergeld fördert, die Planungssicherheit für Polizeieinsätze erhöht – und somit der Allgemeinheit zugutekommt. Es werden keine personenbezogenen Daten ermittelt.

Zur Vorbereitung einer zukünftigen Teststellung wurden für 24 geplante E-Fahrzeuge Dienststellen in den Bundesländern Wien, Niederösterreich, Salzburg und Tirol ausgewählt. Abbildung zeigt die E-Fahrzeuge für den Einsatz in der Teststellung. Um ein möglichst breites Spektrum an Testkriterien abzudecken, wurden Dienststellen mit diversen Sachbereichsschwerpunkten ausgewählt.

Abb.: Für die Polizei folierte E-Fahrzeuge für den Einsatz in der Teststellung

Neben einer Betrachtung von Fahrzeugen und Dienststellen wurden auch mögliche Ladeinfrastrukturlösungen erarbeitet und das Photovoltaik-Potenzial im Hinblick auf eine Blackoutvorsorge evaluiert. Im Zuge dessen wurde ermittelt, dass mit rund 17.065 m² verfügbarer Fläche für Photovoltaikanlagen ein Photovoltaik-Potenzial von 3,8–4,1 Millionen kWh besteht.

Für zukünftige Evaluierungen wurden Simulationen in einem Lade-Park durchgeführt und Ladespitzen analysiert. Wenn die Polizei in Zukunft ihren Fuhrpark mit einer großen Anzahl von E-Fahrzeugen erweitert, werden ein dediziertes Lademanagement und eine Priorisierung der Ladung gewisser Fahrzeuge im Falle einer kW-Begrenzung angeraten. In der Analyse wurden 50 Fahrzeuge in einem Fuhrpark mit Leistungen von 22 kW und 50 kW pro Ladeeinheit angenommen. Bei einer 100-kW-Begrenzung wurden nur wenige Ladevorgänge verzögert. Für die geplante Teststellung wird ein Lademanagement aber aktuell nicht nötig sein, da nur ein bis zwei Fahrzeuge pro Dienststelle stationiert sein werden.

Zur Ausrollung der Teststellung ist es nötig, dass die Fahrzeuge an der Dienststelle laden können. Dafür wurden drei Pakete (11 kW, ≤50 kW-, ≥150 kW) geschnürt, Vorschläge für Komponenten unterschiedlicher Hersteller definiert und in Frage kommenden Dienststellen zugeordnet. In manchen Fällen muss öffentlich geladen werden, wenn z. B. das Laden bei der Dienststelle nicht möglich ist. Daher wurden Kooperationen mit Ladeanbietern oder Gemeinden initiiert. Zudem verfügt jedes Fahrzeug über eine Routex-Karte für das öffentliche Laden.

Um die Umstellung auf Elektromobilität so sicher wie möglich zu gestalten und die Einsatzbereitschaft jederzeit zu gewährleisten, müssen Fahrzeug sowie Infrastruktur robust gegen Cyberattacken sein. Dazu wurde eine Bedrohungsanalyse durchgeführt. Es wurden diverse kritische Angriffsvektoren gegen das Fahrzeug, die Supply Chain und die Ladesäulen identifiziert. Des Weiteren wurden Empfehlungen formuliert, wie diese besser geschützt werden können. Als Beispiel lässt sich hier die Absicherung von Schnittstellen am Fahrzeug und der Ladeinfrastruktur und somit eine bereits vom Hersteller reduzierte Angriffsoberfläche nennen.

Bei einer Polizeiorganisation wurde die Elektromobilität bisher noch nie vollumfänglich – d. h. ohne Einsatzbeschränkungen im Polizeidienst – getestet. Daher wurden Anwendungsfälle definiert, um Grenzbereiche auszuloten und in einer zukünftigen Teststellung praxisnah zu evaluieren. Fahrzeuge müssen ein sicheres Fahrverhalten aufweisen und einem Extrembetrieb möglichst lange standhalten. Keinesfalls darf der Einsatz gefährdet und somit die Sicherheit der Bevölkerung beeinträchtigt werden.

Diese Studie bildet die Grundlage für die Durchführung einer wissenschaftlich begleiteten Teststellung unter Einbeziehung praxisrelevanter Grenzbereiche. Sowohl Fahrzeug(-batterie) als auch Ladeinfrastruktur bedürfen einer dedizierten Untersuchung, um für die Eingliederung einer größeren Menge an Fahrzeugen in die Flotte der Polizei vorbereitet zu sein und passende Handlungsstrategien parat zu haben.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Bundesministerium für Inneres
- Bundesimmobiliengesellschaft m.b.H.
- Porsche Austria GmbH & Co OG
- MOON POWER GmbH
- Wien Energie GmbH

Kontakt:

Martin Latzenhofer
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4134
Mail: martin.latzenhofer@ait.ac.at
www.ait.ac.at

DIGDOK

Innovation durch die Digitalisierung analoger gefangenenbezogener Dokumentationsprozesse im Strafvollzug

Ziel des Projekts DIGDOK (Digitalisierung analoger gefangenenbezogener Dokumentationsprozesse im Strafvollzug) war es, zwischen September 2021 und März 2023 den Status gefangenenbezogener Dokumentationsprozesse mit Fokus auf deren Digitalisierungs- und Automatisierungspotenzial in Justizanstalten zu erheben und diese im Zuge der Umsetzung eines Technology Spikes[1] zu evaluieren. Dazu wurden zwei Justizanstalten ausgewählt, die sich in Größe, Vollzugsform und Modernisierungsgrad unterscheiden, um mit den Ergebnissen bundesweit gültige Aussagen in Bezug auf das Digitalisierungspotenzial treffen zu können.

Methodisch wurde ein offener Feldzugang gewählt, um am Digitalisierungsbedarf und den Problemdefinitionen der Strafvollzugsbediensteten vor Ort anzusetzen. Für die Zusammenführung der technischen und sozialwissenschaftlichen Analysen und Ergebnisse orientierte sich der zyklische Forschungsprozess an der Methode der Situational Analysis[2]. Die Erhebungen fanden innerhalb der qualitativen Feldbeobachtungen in multiperspektivischen Fokusgruppen, Interviews mit Expertinnen und Experten vor Ort und Begehungen der Justizanstalten statt. Der Fokus richtete sich dabei auf sicherheitsrelevante Routinetätigkeiten entlang gefangenenbezogener Dokumentationen.

Die insgesamt neun erhobenen Arbeitsprozesse wurden mit Business Process Model and Notation (BPMN) modelliert. Die bei den Tätigkeiten verwendeten analogen Dokumente wurden wie die modellierten Prozesse gelistet und mittels Vergleichs und Kontrastierung analysiert. Nach der Prozesserhebung wurden Fokusgruppen im Rahmen von Workshops zur Technologiebetrachtung durchgeführt, um den Bedarf und die Akzeptanz der Organisation für geeignete Technologien zu erheben. Als Resultat des Vergleichs konnten die Digitalisierungspotenziale analoger Dokumentationsformen aufgezeigt werden. Anhand der Erhebungsergebnisse wurde ein Use-Case-Diagramm erstellt, woraus drei Use Cases zur weiteren Bearbeitung ausgewählt wurden. Daraus wurde der Use Case „Haftraumdurchsuchung dokumentieren“ als Technology Spike mittels einer mobilen Anwendung entwickelt. Der Testlauf fand von Mitte Dezember 2022 bis Mitte Jänner 2023 statt. Die Evaluierung erfolgte mittels Fragebogen und ergänzenden Interviews mit Bediensteten vor Ort. In einer anwendungsbezogenen Roadmap wurden

---

1 Ein Technology Spike ist eine Aktivität zur Erforschung eines Problems und möglicher Lösungen während der Bereitstellung eines Produkts oder einer Plattform, um eine tatsächliche produktive Umsetzung besser einschätzen zu können.

2 Clarke, Adele E. (2003): Situational Analyses: Grounded Theory Mapping After the Postmodern Turn. In: Symbolic Interaction, Volume26, Issue4, November 2003, Pages 553-576.

die daraus gewonnenen sozialwissenschaftlich-technischen Ergebnisse zusammengeführt, als Lösungsszenarien zur Digitalisierung beschrieben und im Ergebnisbericht dokumentiert.
Die Ergebnisse des Projekts liefern eine empirisch basierte Auswahl der möglicherweise zu digitalisierenden Prozesse. Sie enthalten jene Prozesse, die für eine Digitalisierung aus organisationsspezifischer Perspektive besonders geeignet sind, um die Diversität in der konkreten Durchführung standardisierter Workflows in den verschiedenen Justizanstalten zu berücksichtigen.

Die Anwendung der digitalen Haftraumdurchsuchung mittels mobilen Devices ist in den Arbeitsalltag der Justizwachebeamtinnen und -beamten integrierbar. Aus technischer Sicht sind der automatisierte Datentransfer sowie Datenimport und -export als auch Schnittstellen zu Fachanwendungen für eine Implementierung notwendig. Geschlechts- und altersspezifische Aspekte, Faktoren der Technologieakzeptanz und organisationsspezifische Anforderungen sind zu berücksichtigende Merkmale, um die Bedürfnisse der Endnutzerinnen und Endnutzer im Zuge der Digitalisierung miteinzubeziehen.
Werden die erhobenen Prozesse, der Einsatz von Hardware und Technologie und die Bedürfnisse der Endnutzerinnen und Endnutzer zusammengeführt, ermöglicht das, die Integration weiterer Use Cases und damit die sukzessive Digitalisierung des Strafvollzugs nachhaltig zu planen. Kennzahlen, welche für das Management der Justizanstalten von Relevanz sind, können langfristig natürlich aus der Anwendung von Applikationen im Zuge von täglichen Routineabläufen generiert werden.

Projektleitung:

Vienna Centre for Societal Security Research GmbH (VICESSE)

Projektpartner:

- Bundesministerium für Justiz
- Verein Fachhochschule Technikum Wien (FHTW)

Kontakt:

Marion Neunkirchner BA MA
Vienna Centre for Societal Security (VICESSE)
Paulanergasse 4/8
1040 Wien
Tel: +43 1 929 66 38
Mail: marion.neunkirchner@vicesse.eu
www.vicesse.eu

DigitRes

Digital unterstützte Resozialisierung im Strafvollzug

In diesem Projekt werden die Grundlagen für eine sichere Ausweitung des Zugangs von Inhaftierten bzw. Untergebrachten zu modernen Informations- und Kommunikationstechnologien im österreichischen Strafvollzug erarbeitet. Bedarfsträger ist das Bundesministerium für Justiz. Mit Herbst 2023 startet ein mehrmonatiges Pilotprojekt in einer ausgewählten Justizanstalt, in der Inhaftierte beschränkten Zugang zu digitalen Geräten erhalten. Im Vorfeld des Modellprojekts wurden bereits sozialwissenschaftliche Grundlagen für dessen Implementierung erarbeitet. In einem ersten Schritt wurde im Rahmen einer qualitativen Befragung der Bedarf von Inhaftierten hinsichtlich digitaler Geräte erhoben. Insgesamt wurden 39 Interviews mit Inhaftierten sowie ehemalig langzeitinhaftierten Personen geführt. Ziel der Interviews war es, einen Einblick in die Erfahrungen und Bedürfnisse von Inhaftierten österreichischer Justizanstalten hinsichtlich der Nutzung von digitalen Geräten zu erhalten. Im Gespräch mit Haftentlassenen wurde außerdem erhoben, ob und inwiefern sie durch mangelnde digitale Kompetenzen Probleme bei der Wiedereingliederung in die Gesellschaft hatten und wie ihnen ein ausgeweiteter Zugang zu digitalen Geräten in Haft bei der Reintegration hätte helfen können.

Neben der Bedarfserhebung wurden zusätzlich Gespräche mit 15 Expertinnen und Experten aus den Bereichen Anstaltsleitung, Vollzugsleitung, IT-Leitbedienung, Fachdienste, Bildung/Ausbildung und Datenschutz geführt, um professionelle Einschätzungen hinsichtlich der Chancen und Risiken der Digitalisierung des Strafvollzugs sowie Tipps für die praktische Umsetzung des Modellprojekts zu erhalten. In Vorbereitung des Pilotprojekts wurden zudem die diversen internationalen Anbieter digitaler Geräte für Inhaftierte verglichen sowie Vorerfahrungen zur Bereitstellung digitaler Geräte für Inhaftierte eingeholt. Um einen Einblick in die Einschätzung des Strafvollzugspersonals zu erhalten, wurde schließlich eine österreichweite Online-Befragung durchgeführt, an der 604 Personen teilnahmen. Auch wenn das Projekt DigitRes noch nicht abgeschlossen ist, können an dieser Stelle erste Erkenntnisse präsentiert werden.
Viele Inhaftierte sahen die Ausweitung des Zugangs zu digitalen Geräten als Möglichkeit, mehr Selbstständigkeit und Autonomie zu erhalten und ihre Zeit in Haft sinnvoller nutzen zu können. Ein großer Teil der Befragten befürwortete die Digitalisierung administrativer Prozesse, den Zugang zu digitalen Bildungs-, Unterhaltungs- und Informationsangeboten sowie eine mögliche Ausweitung der Kommunikationsmöglichkeiten mit der Familie. Gerade im Bereich der Entlassungsvorbereitung attestierten viele der Digitalisierung und den damit verbundenen Möglichkeiten großes Potenzial. In den Gesprächen wurden auch Risiken und Hürden benannt, die mit der Ausweitung des Zugangs zu digitalen Geräten einhergehen können. Diese reichten von möglichem Missbrauch und Beschädigungen der Geräte bis zu dem potenziellen Verlust wichtiger sozialer Interaktionen. Auch die zum Teil mangelnden sprachlichen,

kognitiven und digitalen Fähigkeiten von Inhaftierten wurden im Rahmen der Gespräche benannt sowie der deshalb notwendige Betreuungsaufwand, der zumindest in der Anfangszeit das Justizwachepersonal zusätzlich belasten könnte.

Unabhängig von der Stellung im System Strafvollzug sahen die interviewten Expertinnen und Experten in der bedarfsorientierten Digitalisierung das Potenzial, die Resozialisierung zu unterstützen, das System Strafvollzug zu modernisieren, die Haftbedingungen für Inhaftierte zu verbessern und deren Rechte zu stärken sowie auf Dauer die Entlastung des Personals durch die Entbürokratisierung analoger Prozesse zu befördern. Zugleich wurden Risiken und Herausforderungen der Digitalisierung genannt, die bei der Implementierung berücksichtigt werden müssen – vom personellen und finanziellen Ressourcenaufwand über die baulichen und technischen Rahmenbedingungen, die Missbrauchsgefahren und möglichen Beschädigungen bis hin zu möglichen Akzeptanzproblemen beim Personal bzw. der Öffentlichkeit. Trotz der genannten Risiken befürworteten die Expertinnen und Experten einhellig die Digitalisierung des Strafvollzugs.

Die Online-Befragung des Strafvollzugspersonals brachte einige überraschende Ergebnisse, die als Ergänzung zur Bedarfserhebung und den Experteninterviews in die Planung und Umsetzung des Modellprojekts einfließen. Die Ausweitung des Zugangs zu digitalen Geräten für Inhaftierte erfuhr mehr Zustimmung als erwartet. Nur eine kleine Personengruppe sprach sich grundsätzlich gegen Digitalisierungsmaßnahmen aus. In bestimmten Bereichen stimmte ein großer Teil der Ausweitung zu – das betraf vor allem die Ausweitung der Bildungs- und Ausbildungsinhalte, die Entlassungsvorbereitung sowie die digitale Unterstützung in der Kommunikation mit fremdsprachigen Inhaftierten. Zugleich wurde die Digitalisierung bestimmter Bereiche kritisch bewertet, etwa die interne Kommunikation über Messenger und Videotelefonie, der Einblick in den eigenen Akt oder auch das Ansuchen- und Beschwerdewesen.
Auf der Basis dieser empirischen Ergebnisse und eines Workshops zur kooperativen Wissensbildung, bei dem die relevanten Stakeholder aus dem Bundesministerium für Justiz und der Anstalt, in der das Modellprojekt stattfindet, eingebunden sind, und unter Berücksichtigung internationaler Erfahrungen wird ein konkretes Modellprojekt definiert. Im Rahmen der sozialwissenschaftlichen Begleitforschung wird schließlich die Umsetzung des Modellprojekts laufend evaluiert, um wichtige Erkenntnisse zur Digitalisierung des Strafvollzugs generieren zu können.

Projektleitung:

Universität Innsbruck

Projektpartner:

- Bundesministerium für Justiz

Kontakt:

Veronika Hofinger
Universität Innsbruck
Museumstraße 5/12
1070 Wien
Tel: +43 512 507 73905
E-Mail: veronika.hofinger@uibk.ac.at
www.uibk.ac.at/irks/

EASIER

Enabling and Assessing Trust when Cooperating with Robots in Disaster Response

Die strategischen Ziele des Projekts umfassen folgende Aspekte. Der Hauptaspekt des Projektes ist die Förderung des praktischen Einsatzes von Assistenzrobotern durch Einsatzorganisationen. Zentrales Ziel ist hier der verbesserte Schutz der Einsatzkräfte, die nicht direkt im Gefahrenbereich arbeiten müssen, bzw. die Verbesserung des Lagebilds. Durch Interviews mit Einsatzkräften ist allerdings evident, dass vollautonome Systeme momentan weder der Akzeptanz durch die Einsatzkräfte noch dem Stand der Technik nach realistisch einsetzbar sind. Das Projekt fokussiert sich daher auf teilautonome Robotersysteme, bei denen das Ausmaß der Autonomie im Zusammenspiel zwischen Einsatzkraft und Roboter adaptiert werden kann. Für die Akzeptanz von Assistenzrobotern ist das Vertrauen der Einsatzkräfte in das System von größter Bedeutung. Daher ist ein strategisches Ziel des Projektes, das Vertrauen in Assistenzroboter bei den Einsatzkräften zu erhöhen. Um dies zu erreichen, wird im Projekt an Ansätzen von „Shared Autonomy“ für die Anwendung in der mobilen Manipulation gearbeitet.

Die wissenschaftlichen Ziele des Projekts beinhalten einerseits die Entwicklung neuer Methoden zur Messung des Vertrauens in Robotersysteme und andererseits erweiterte Roboterfähigkeiten, die das Vertrauen erhöhen sollen. Im Rahmen des Projektes werden neuartige nicht invasive Methoden zur Messung von Vertrauen und kognitiver Belastung entwickelt, da klassische Methoden mit Fragebögen den Ablauf eines Einsatzes stören und die Ergebnisse verfälschen können. Zur Steigerung des Vertrauens werden aufgabenspezifischen Konzepte für die Benutzerschnittstelle entwickelt. Neben dem Format und Daten der Ausgaben sowie der Steuerelemente wird auch der Autonomiegrad in der Mensch-Roboter-Interaktion situationsabhängig automatisch angepasst. Ferner wird an der Erhöhung des Transparenzgrades des Roboters gearbeitet, indem der Roboter transparente Erklärungen zu seinen Entscheidungen, Aktivitäten und Fehlern liefert.

Eine Übersicht des Systems ist in der nachfolgenden Grafik dargestellt. Die Einsatzkraft bedient den Assistenzroboter mittels einer Benutzerschnittstelle, wobei nahtlos zwischen Teleoperation und automatisierten Funktionen gewechselt werden kann. Der Roboter selbst liefert Erklärungen für sein Verhalten, triggert Adaptionen der Benutzerschnittstelle und wechselt automatisch zur passenden Autonomiestufe. Zum Beispiel gibt der Roboter die Kontrolle an den Benutzer zurück, wenn eine Aufgabe nicht mehr zuverlässig ausgeführt werden kann.

Zentrale Aspekte der Benutzerschnittstelle sind, dass sie sich selbst an die aktuelle Aufgabe und Autonomiestufe anpasst und transparent den mentalen Zustand des Roboters kommuniziert. Zusätzlich werden für eine effiziente Zusammenarbeit mit dem Roboter templatebasierte Interaktionsmethoden entwickelt. Beim Öffnen einer Tür zeigt der Benutzer nur auf die Scharniere und die Klinke einer Tür und der Roboter versteht, wie eine spezielle Tür zu öffnen ist.

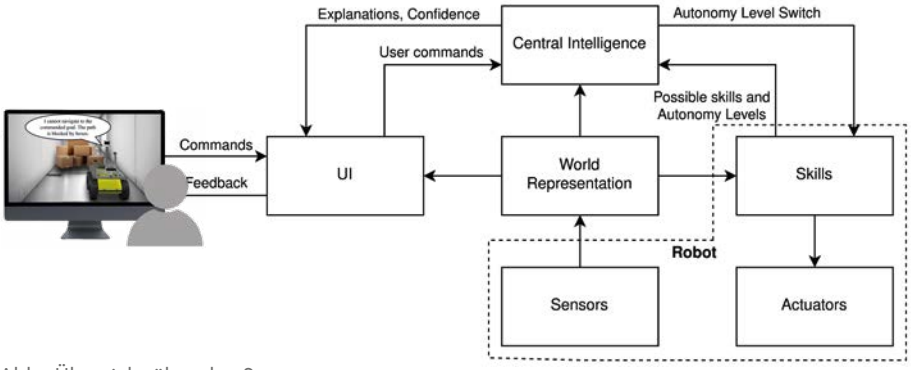


Abb.: Übersicht über das System

Im Rahmen des Transparenz-Moduls liefert der Roboter verbale SAT-Erklärungen, um den Benutzer über seine Planung, Zustand und Aufgabenzuversicht sowie über getroffene Entscheidungen und das Ergebnis der Aufgabe (Erfolg, Misserfolg) zu informieren. Diese transparenten Erklärungen sollen das Vertrauen in Robotersysteme erhöhen und die kognitive Belastung bei der Bedingung vermindern.

Folgende Anwendungsfälle wurden berücksichtigt, die eine Hierarchie von Fähigkeiten zur Bewältigung von Katastrophenschutzaufgaben bilden. Ebene 0 umfasst Situationswahrnehmung und Navigation mittels geometrischen und semantischen Mappings, automatisierte Wegpunkt-Navigation und die Detektion und Klassifizierung von Hindernissen. Ebene 1 umfasst das Freimachen von Wegen mittels Unterstützung des Roboters bei der Navigation in schwierigen Situationen, das Beseitigen von Trümmern und das Öffnen von Türen. Ebene 2 umfasst die Manipulation von Vorrichtungen aus der Ferne und die Betätigung von Ventilen und Hebeln. Ebene 3 umfasst die Manipulation von Behältern zur sicheren Beseitigung von Gefahrstoffen an kritischen Stellen.

Für die Evaluierung der entwickelten Methoden wurden zwei Experimente mit multifaktoriellen und multivariaten Designs mit wiederholten Messungen durchgeführt. Dafür mussten vorwiegend Einsatzkräfte in einer kontrollierten Laborumgebung Navigations- und Manipulationsaufgaben mit einem Assistenzroboter lösen. Hier wurde ein nicht invasiver mehrstufiger Ansatz gewählt und es wurden subjektive (Selbstberichte, Bewertungen) und objektive (Psychophysiologie, Leistung) Daten gesammelt.

Um verschiedene Ansätze zur Transparenz, Benutzerschnittstelle und Autonomiestufe zu untersuchen, wurden die Experimente mit Kontroll- und Behandlungsgruppen durchgeführt. Eine Bewertung des Vertrauens und kognitiver Belastung sowie der entsprechenden HMI-Faktoren (Benutzerfreundlichkeit, Zufriedenheit, VR-Krankheit) wurde ebenfalls durchgeführt. Erste Ergebnisse der Auswertung der Experimente haben gezeigt, dass das innovative transparente Konzept der Mensch-Roboter-Kollaboration zur Steigerung des Vertrauens von Einsatzkräften führt. Diese Ergebnisse können die Basis für eine breitere Verwendung von Assistenzrobotern durch Einsatzkräfte bilden.

Projektleitung:

Technische Universität Graz

Projektpartner:

- Berufsfeuerwehr Graz
- Bundesministerium für Landesverteidigung
- Disaster Competence Network Austria
- Institut für Psychologie, Universität Graz
- Institut für Maschinelles Sehen und Darstellen, Technische Universität Graz
- Rosenbauer International AG

Kontakt:

Prof. Dr. Gerald Steinbauer-Wagner
Technische Universität Graz
Inffeldgasse 16b/2
8010 Graz
Tel: +43 316 873 5723
E-Mail: steinbauer@ist.tugraz.at
www.tugraz.at/institutes/ist/

e-Panini

Elektronische Plattform eines Bezugsberechtigungssystems für Güter, Produkte und Dienstleistungen

Um in Krisenfällen die Versorgung der Bevölkerung mit lebensnotwendigen Gütern als auch Dienstleistungen und in zweiter Linie der Unternehmen mit notwendigen Vorprodukten (Roh-, Halb- und Fertigfabrikate) langfristig zu gewährleisten, bedarf es bei kritischen Versorgungsengpässen und einem Versagen der üblichen Marktmechanismen eines belastbaren und fälschungssicheren Verteilungssystems. Nach über 50 Jahren soll dieses grundsätzlich noch vorhandene System der Bezugsberechtigungen in Papierform („Lebensmittelmarken“) durch ein neues digital unterstütztes Framework ersetzt werden.

Dazu ist es erforderlich, ein grundlegendes Konzept für Bezugsberechtigungen auf Basis von Informations- und Kommunikationstechnologie (IKT) und den dafür geeigneten technologischen Bausteinen zu erarbeiten. Dies zum Anlass nehmend, müssen die aktuellen Normbedarfe aus den 1950er- und 1960er-Jahren neu gestaltet und angepasst werden, sei es bei Lebensmitteln, Hygieneprodukten, Medizin- und Arzneibedarf oder Dienstleistungen im Rahmen der Deckung von Grundbedürfnissen, differenziert nach Kriterien der Endverbraucherinnen und Endverbraucher. Diese unterscheiden sich durch die unterschiedlichen Berufe (Schwer- bis hin zu Büroarbeit), Lebenssituation (Armutsgefährdung, Mittelstand, Altersstruktur, soziales Umfeld), Region (Stadt, Land, alpiner Bereich) etc.

Außerdem ist festzulegen, welche Güter und Dienstleistungen als kritisch gesehen werden, ob es mögliche Substitute geben kann, wie deren Durchhaltedauer respektive Lagerfähigkeit gestaltet ist. Es muss in wirtschaftlichen Mangellagen möglich sein, verschiedene ähnliche Produkte als ein generelles Gut zusammenzufassen – sei es durch den Hersteller als auch durch den Einzelhandel. Auch Verpackung als orthogonaler Faktor oder Logistik sind dabei zu berücksichtigen. Hier kann ein wohldosiertes Instrumentarium an etwaigen Lenkungsmaßnahmen für die Ministerien mit Wirtschaftslenkungskompetenz helfen, die Versorgung der Bevölkerung sicherzustellen. Das IKT-Bezugsberechtigungskonzept soll flexibel für verschiedenste Katastrophen- und Krisenszenarien (z. B. Blackout, Internetausfälle, vernetzte Krisen) einsetzbar sein und im Falle von wirtschaftlichen Mangellagen eine möglichst faire und effiziente Verteilung von Gütern und Dienstleistungen sicherstellen. Ein derartiger Ansatz erlaubt theoretisch eine bedarfsangepasste rasche Kontingentierung, Abstimmung auf die aktuellen Bedürfnisse der Bevölkerung und der Unternehmen sowie eine Steuerung und Monitoring in Echtzeit, wenn anverwandte IKT-Systeme wie Distributions- und Logistiksysteme, Lagerbewirtschaftungen und Verteilungssysteme angebunden werden können.

Das Bezugsscheinsystem soll in bestehende und zu entwickelnde Organisationen so eingebunden werden, dass das System in – möglicherweise langen – Phasen des Nicht-Betriebs aktuell und einsatzfähig gehalten werden kann und ein schnelles Umschalten in den Betriebsmodus gewährleistet ist. Es wird

erörtert, wie das IKT-Bezugsberechtigungskonzept in die öffentliche Verwaltung, insbesondere bei den für Wirtschaftslenkung verantwortlichen Bundesministerien, sowie in die föderalen Verwaltungsstrukturen eingebettet und sicher betrieben werden kann.

Neben diesen Vorteilen entstehen andererseits allerdings neue Risiken bei der Einführung eines digitalen IKT-Konzepts. Es muss missbrauchs- und fälschungssicher gestaltet sein, Security-by-Design-Prinzipien folgen und dennoch typische Anwendungsfälle des Systems berücksichtigen (z. B. Tausch von Bezugsberechtigungen, Verwendung von Bezugsscheinen für jemand anderen, o. Ä.). Neben einer resilienten und redundanten Ausgestaltung muss auch ein temporärer Offline-Inselbetrieb ermöglicht werden, insbesondere bei großflächigem IKT-Ausfall, und danach eine konsistente Datensynchronisation gewährleistet werden. Aus den Erfahrungen der Pandemie wird in diesem Projektvorhaben explizit auch die Frage nach den gesellschaftlichen und sozialen Faktoren gestellt. Neben Gestaltungsfragen, wie ein solches digitales Konzept von möglichst allen Bevölkerungsteilen verwendet werden kann.

Ein solches IKT-Bezugsberechtigungskonzept verbindet somit die Anforderungen (der Bevölkerung) mit den Produktionspotenzialen (der Hersteller), den bereits vorhandenen Produktmengen (der Lieferanten und Verteiler) und berücksichtigt auch deren Veränderungen über die Dauer der wirtschaftlichen Mangellage und bezieht aktuelle Rahmenbedingungen (soziale Verhaltensweisen, Logistik) ein. Es bildet einen wesentlichen Baustein in der Modernisierung der wirtschaftlichen Krisenvorsorge.

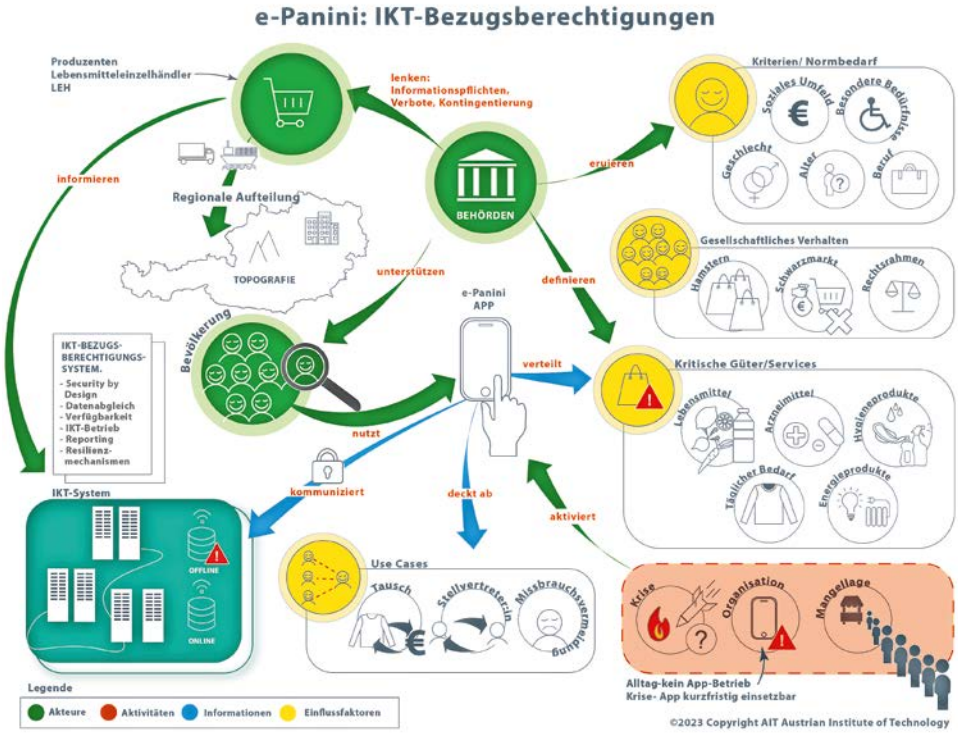


Abb.: Übersicht über die Plattform für IKT-Bezugsberechtigungen

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Stadt Wien
- Land Tirol
- Fraunhofer Austria Research GmbH
- Universität Linz
- Bundesanstalt Statistik Österreich
- Dipl.-Ing. Dr. Hermann Bühler GmbH
- Österreichische Gesellschaft für Ernährung
- Österreichischer Zivilschutzverband
- Kammer für Arbeiter und Angestellte für Wien
- youniqx Identity AG

Kontakt:

Martin Latzenhofer
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4134
Mail: martin.latzenhofer@ait.ac.at
www.ait.ac.at

EPISTEMIS

Epistemische Sicherheit. Zur Rolle wissenschaftlicher Expertise in chronischen Krisen

Programmschwerpunkt 3.2.9: „Krisenmanagement in nationalen und globalen Krisen und die Rolle von Wissenschaft und Forschung“

Die Covid-19-Pandemie stellte die Politik weltweit vor die Herausforderung, Entscheidungen unter großen Unsicherheiten zu treffen. Dabei wurde die Wissenschaft in den meisten europäischen Staaten zur Mitstreiterin: Sie arbeitete unter Hochdruck, um Daten und Zusammenhänge zu generieren, und half damit, Unsicherheiten zu reduzieren und politische Entscheidungen zu informieren.
Damit stellt sich die grundlegende Frage: Wie kann die Politik in der Krise beraten werden? Was kann die Wissenschaft in Situationen von Unübersichtlichkeit und Zeitdruck als Beraterin leisten? Und welchen Bedarf an Beratung sieht die Politik für sich selbst?
Um diese Frage zu beantworten, untersuchte das Projekt EPISTEMIS wissenschaftliche Politikberatung in drei europäischen Ländern: Österreich, Großbritannien und Deutschland. Diese unterschieden sich nicht nur bezüglich ihrer politischen Strategien im Umgang mit der Pandemie, sondern auch bezüglich ihrer Beratungsstrukturen.
Großbritannien und Deutschland verfügten bereits über etablierte wissenschaftliche Beratungssysteme, während sich ein solches in Österreich erst im Verlauf der Pandemie professionalisierte. In Großbritannien übersetzt ein Sekretariat der Regierung politische Fragen in wissenschaftliche, zu denen Fachgremien Evidenzen erarbeiten. Ein übergeordnetes Beratungsgremium (Scientific Advisory Group for Emergencies – SAGE) gewichtet diese und formuliert Empfehlungen für die Politik. In Deutschland forscht und berät die Ressortforschung (genauer: Robert Koch-Institut – RKI) zu Infektionskrankheiten. Gleichzeitig meldeten sich unabhängige Beratungsgremien wie Leopoldina oder Deutscher Ethikrat zu Wort. In Österreich befassten sich verschiedene Gremien mit Covid-19, deren Zuständigkeiten sich im Verlauf der Pandemie ausdifferenzierten. Die Gesamtstaatliche Covid-Krisenkoordination (GECKO), im Dezember 2021 einberufen, zentralisierte letztendlich die wissenschaftliche Politikberatung in Österreich. Ende März 2023 löste sie sich vorzeitig auf.

Wesentliche Projektergebnisse:

- Für die Vorbereitung auf zukünftige Krisen sind etablierte Beratungsstrukturen entscheidend. Das deutsche RKI hat beispielsweise durch seine finanzielle und personelle Ausstattung die Möglichkeit, Expertise durch Forschung zu konkreten politikrelevanten biomedizinischen Fragen zu unterfüttern. Auch in Großbritannien hat SAGE über nachgereihte Fachgruppen die Möglichkeit, Evidenzen generieren zu lassen.

- Herrschende Problemformulierungen und deren Rahmen (Framing) sind entscheidend dafür, welche Disziplinen, Informationen und Maßnahmen als relevant gelten. Wissenschaftliche Perspektiven, die sich nicht innerhalb dieses Rahmens bewegen, haben einen schweren Stand. Für die Politikberatung gilt das genauso: Das Problem-Framing bestimmt, welche Expertinnen und Experten zurate gezogen werden. Es ist eine wichtige Aufgabe wissenschaftlicher Beratung, das vorherrschende Framing zu reflektieren. Ob die Pandemie vorrangig als Gesundheits- oder Sozialproblem verstanden wird, beeinflusst in großem Maße, welche Disziplinen als (beratungs-)relevant und welche Maßnahmen als legitim gelten.
- Konsens unter den Mitgliedern eines Expertengremiums wurde von der politischen Seite häufig gelobt. Allerdings ist Konsens kein automatisches Produkt von Gremien, er muss vielmehr aktiv durch institutionelle und organisatorische Vorkehrungen ermöglicht werden. Dies geschah in den untersuchten Gremien durch entsprechende Expertenauswahl oder ein Problem-Framing, das Grundsatzdiskussionen über Disziplingrenzen hinweg ausschloss oder durch Abstraktionshöhe der Themen grundlegenden Dissens vermied. Konsens ist jedoch kein Selbstzweck und verhindert oft eher die Reflexion über das Problem-Framing – im extremsten Fall kann er sogar als Legitimationsressource für eine Politik der Alternativlosigkeit dienen. Ein gehaltvoller Dissens unter namhaften Expertinnen und Experten kann hingegen unterstreichen, dass die Entscheidungsmacht letztendlich bei der Politik verbleibt.

Empfehlungen für wissenschaftliche Politikberatung in Krisen:

- Beratung sollte Optionen anbieten: Die Wissenschaft sollte sich in der Rolle eines „ehrlichen Maklers“ (Roger Pielke) sehen, der der Politik Entscheidungsalternativen auf Basis wissenschaftlicher Evidenz und Expertise aufzeigt. Wissenschaftsbasierte Beratung sollte nicht dazu dienen, der Politik die Begründungslasten abzunehmen oder Entscheidungen ex-post zu legitimieren.
- Beratung muss nicht konsensual sein: Eine nur dissonante Wissenschaft ist keine Hilfe in Krisenzeiten. Ein institutionell von vornherein sichergestellter Konsens verhindert aber die wertvolle Möglichkeit zur Reflexion von Problemstellungen. Außerdem besteht die Gefahr, dass die Wissenschaft auf diese Weise die Politik nicht vor allem informiert, sondern vorrangig zu Legitimationszwecken dient.
- Beratung muss ihr Framing reflektieren: Unter welcher Problemformulierung Beratung geschieht, ist entscheidend für die mobilisierte Expertise. Unterschiedliche Perspektiven können wertvolles Wissen einbringen, hierfür muss jedoch epistemischer und organisatorischer Platz geschaffen werden – jenseits von eindimensionaler Problemformulierung.
- Beratung braucht systematische Unterstützung: Für die notwendige Evidenzbildung sowie wissenschaftliche Begleitung politischer Interventionen müssen Ressourcen bereitgestellt werden, um belastbare Erkenntnisse generieren zu können. Hier bieten sich eigene Evidenzbildungsapparate an, wie sie aus Großbritannien (SAGE) und Deutschland (RKI) bekannt sind.

Projektleitung:

ÖAW – Institut für Technikfolgen-Abschätzung

Projektpartner:

- Bundesministerium für Landwirtschaft, Regionen und Tourismus

Kontakt:

Alexander Bogner
Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften (ÖAW)
Apostelgasse 23
1030 Wien
Tel: +43 1 51581 6595
E-Mail: abogner@oeaw.ac.at
www.oeaw.ac.at/ita/

ESBH

Effiziente, sichere bauliche Haftgestaltung in Justizanstalten in Österreich

ESBH wurde im Herbst 2022 gestartet. Im Projekt ist geplant, auditierbare baulich-technische Standards auf Basis von sozialer, wirtschaftlicher und ökologischer Nachhaltigkeit zu entwickeln. Diese sollen helfen, Sicherheit, Betreuungsqualität und das Erreichen der Vollzugsziele in Justizanstalten zu unterstützen.

Trotz ständiger Modernisierungsmaßnahmen stellt die starke bauliche Diversität der österreichischen Justizanstalten eine Herausforderung für die Umsetzung von einheitlichen Standards dar, die den Bedürfnissen aller Nutzerinnen und Nutzer (Anstaltsleitung, Beschäftigte sowie Insassinnen und Insassen) entsprechen. Das interdisziplinäre Projektteam unter der Leitung der beiden Fachbereiche Risiko- und Sicherheitsmanagement und Architektur – Green Building der FH Campus Wien setzt sich daher im Forschungsprojekt „Effiziente, sichere bauliche Haftgestaltung in Justizanstalten in Österreich“ (ESBH) zum Ziel, nachhaltige baulich-technische Standards zu entwickeln, die auf dem Status quo der 23 Justizanstalten (gerichtliche Gefangenenhäuser und Strafvollzugsanstalten) aufbauen, mit allen relevanten Stakeholdern abgestimmt sind und die Bedürfnisse, Problemlagen und Use Cases aller Nutzergruppen einbeziehen. Die fachübergreifende Kooperation des Projektteams zur Erreichung der Projektziele verläuft erfolgversprechend und im Zeitplan.

Das Projekt ist in vier Arbeitspakete (AP) gegliedert. Im AP 01 (Projektmanagement) erfolgt die Kommunikation und Abstimmung mit Projektpartnerinnen und -partnern sowie der Forschungsförderungsgesellschaft. Im AP 02 (Grundlagenphase; bereits abgeschlossen) wurde der Status quo der 23 Justizanstalten hinsichtlich Belagszahlen, Anzahl der Beschäftigten, Organisationsstruktur, baulicher Rahmenbedingungen und Infrastruktur qualitativ und quantitativ beschrieben. Dieses Arbeitspaket lieferte darüber hinaus die relevanten nationalen und internationalen Grundlagen zu den Themen rechtliche Rahmenbedingungen, baulich-technische „Good and best Practices“ sowie systemische und dynamische Sicherheit in Organisationen. Die Studienreisen nach Deutschland (Regensburg), Finnland (Hämeenlinna) und Norwegen (Halden) wurden erfolgreich durchgeführt, die gewonnenen Erkenntnisse fließen in die weitere Arbeit ein. Mit Sommer 2023 (Redaktionsschluss) hat das Team einen umfangreichen Zwischenbericht als Abschluss des AP 02 vorgelegt. Wie die internationale Literatur und die Erkenntnisse aus den Studienreisen zeigen, sind einheitliche strategische Vorgaben zur Umsetzung der Haftziele, um mittel- und längerfristig unterstützende bauliche-technische Standards etablieren zu können, erforderlich. Die Wirkungsziele des Straf- und Maßnahmenvollzuges definieren Faktoren, welche einen effektiven, humanen und sicheren Straf- und Maßnahmenvollzug mit Fokus auf Rückfallprävention und (Re-)Integration sicherstellen. Die Wirkungszusammenhänge sind dabei jedenfalls aus folgenden beispielhaften Interventionen und Tätigkeiten abzuleiten:

Beschäftigung, Forcierung von Bildungsmaßnahmen, Wiederherstellung und Erhaltung von physischer und psychischer Gesundheit, Behandlung und Abschwächung von Risikofaktoren, welche das Entstehen von strafbaren Handlungen begünstigen, Unterstützung bei (re-)integrativen Maßnahmen aller Art, Vermittlung von Struktur und von allgemein gesellschaftlich anerkannten Werten und Haltungen, Allgemeinversorgung und Gewährleistung eines sicheren Straf- und Maßnahmenvollzuges sowie Forcierung von modernen Haftformen, sodass Integration erhalten bleibt und Kollateralschäden und zusätzliche Kosten für die Gesellschaft vermieden werden. Aufgrund dieser Vielzahl an Einflussfaktoren auf die Wirkungsziele und deren komplexer Wirkungsweise zueinander und der großen Diversität der baulichen Struktur der Landesgerichtlichen Gefangenenhäuser bzw. Strafvollzugsanstalten ist es derzeit schwierig, letztgültige Empfehlungen für baulich-technische Standards für JA zu entwickeln.

Weitere Hinweise sind darüber hinaus in internationalen rechtlichen Vorgaben, dem StVG und dem Abschlussbericht der Arbeitsgruppe „Strafvollzugspaket – NEU/Sichere Wege aus der Kriminalität" (Bundesministerium für Justiz, 2021) zu finden und können für die weitere Vorgehensweise verwendet werden.

In einem nächsten Schritt werden ab Sommer 2023 die in der Stichprobenziehung ausgewählten 9 Justizanstalten im Zuge des AP 03 einerseits mittels sozialwissenschaftlicher Methoden untersucht, andererseits anhand der Bestandspläne und Vorort-Begehungen hinsichtlich baulich-räumlicher und technischer Gegebenheiten analysiert. Hierbei stehen vor allem die Bedürfnisse, Problemfelder und Use Cases der Nutzerinnen und Nutzer (Leiterin/Leiter, Mitarbeiterinnen/Mitarbeiter und Insassinnen/Insassen) im Vordergrund. Die inneren Abläufe (Logistik) werden dokumentiert und aus einer interdisziplinären Perspektive (Soziologie, Architektur, Digitalisierung), welche die bisherigen Projektergebnisse miteinbezieht, ausgewertet und wiederum in einem Ergebnisbericht dargestellt.

Im AP 04 (Analyse- und Ergebnisphase) wird, aufbauend auf den bisherigen Ergebnissen, eine Soll-Ist-Analyse durchgeführt, um nachhaltige baulich-technische Standards abzuleiten. Diese werden mit allen relevanten Stakeholdern abgestimmt und fließen letztlich in einen praxisorientierten Planungskatalog für Auftraggeber und Umsetzende ein, der die Grundlage für ein digitales Zertifizierungstool darstellt. Der Planungskatalog und das anwendungsorientierte Zertifizierungstool ermöglichen sowohl für Auftraggeber (BMJ, BMI, BIG) wie auch für Auftragnehmer eine effizientere und effektivere Durchführung von öffentlichen Ausschreibungen sowie eine raschere und bedarfsgerechtere Umsetzung künftiger Modernisierungsmaßnahmen bei österreichischen Justizanstalten, um vor allem die Exekutivbediensteten und Fachdienste bei ihren zentralen Aufgaben zu unterstützen.

Abb.: Welche Herausforderungen im Strafvollzug bringt die Digitalisierung?

Projektleitung:

FH Campus Wien

Projektpartner:

- Bundesministerium für Justiz
- BIG – Bundesimmobiliengesellschaft
- Bundesministerium für Inneres
- Institut für Rechts- und Kriminalsoziologie
- Linienreich Generalplanung & Projektmanagement GmbH
- app informatics zt gmbh

Kontakt:

FH-Prof.in Mag.a Claudia Körmer
Dipl.-Ing.in Dr.in Hildegard Sint
Fachbereich Risiko- und Sicherheitsmanagement
Fachbereich Architektur – Green Building
FH Campus Wien
Favoritenstraße 226, Raum B.3.10
1100 Wien
Tel: +43 1 606 68 77 2164
claudia.koermer@fh-campuswien.ac.at
www.fh-campuswien.ac.at

Illustrationen:

Auszüge aus der Umfrage bei Führungskräften in österreichischen Justizanstalten (Frühjahr 2023)

evaluating_UNDER18

Evaluationsstudie zur Messung der Umsetzungsqualität und Wirksamkeit des Jugend-Kriminalpräventionsprogramms „UNDER18“

Die Studie „evaluating_UNDER18“ evaluiert das Jugend-Kriminalpräventionsprogramm „UNDER18“, das vom Büro für Kriminalprävention und Opferhilfe des Bundeskriminalamts/Bundesministeriums für Inneres (BM.I) seit 2018 österreichweit angeboten wird. UNDER18 setzt sich aus drei Teilprogrammen mit unterschiedlichen Schwerpunktsetzungen zusammen („Click&Check“, „AllRight“ und „Look@yourLife“) und richtet sich an Jugendliche im Alter von 13 bis 17 Jahren.

In der Umsetzung sind dafür mehr als 400 Jugend-Präventionsbedienstete als Trainerinnen und Trainer im Einsatz. In einer österreichweiten einheitlichen Ausbildung werden wesentliche Aspekte der Entwicklungspsychologie, Gewalt- und Suchtentstehung, Methodik, Didaktik und Kommunikation vermittelt. Außerdem haben die Präventionsbediensteten umfangreiche Schulungsunterlagen inklusive Übungsanleitungen und Arbeitsblätter sowie einen Methodenkoffer zur Verfügung.

Trotz des hohen Potenzials von UNDER18 liegen bislang keine empirischen Daten darüber vor, (1) wie die Teilprogramme von den Präventionsbediensteten qualitativ umgesetzt werden, (2) wie diese von Jugendlichen, Bildungseinrichtungen und Eltern/Erziehungsberechtigten wahrgenommen und bewertet werden, und (3) ob die Programmziele erreicht werden und die beabsichtigte Wirkung zeigen. Dieses Wissen ist nicht nur für das Aufzeigen von Optimierungspotenzialen von UNDER18 unabdingbar, sondern auch entscheidende Bewertungsgrundlage für dessen Qualität als effektives, evidenzbasiertes Jugend-Kriminalpräventionsprogramm.

Das Projekt evaluating_UNDER18 greift diesen Forschungsbedarf auf und setzt auf innovative Weise erstmals eine umfangreiche österreichweite Prozessevaluation (= Prüfung der Implementierungsqualität) und Wirkungsevaluation (= Nachweis der intendierten Wirkung) des polizeilichen Jugend-Kriminalpräventionsprogramms „UNDER18“ um.

Das Forschungsdesign umfasst ein breit angelegtes Methodenrepertoire, das sowohl quantitative Zugänge (österreichweite quantitative Online-Erhebungen von an den Präventionstrainings teilnehmenden Jugendlichen mit quasiexperimentellem Design in mehreren Erhebungswellen) als auch qualitative Methoden (Gruppendiskussionen und Interviews mit Präventionsbediensteten sowie Personen aus dem schulischen Umfeld, Eltern/Erziehungsberechtigte) vorsieht. Die Evaluierung schließt mit der Entwicklung eines begleitenden Monitoring-Tools ab, um die Qualität des Programms langfristig sicherzustellen. Für die Umsetzung dieses aufwendigen Erhebungsdesigns ist eine enge Kooperation mit dem Bundeskriminalamt/BM.I erforderlich, insbesondere betreffend die Unterstützung bei der konkreten Durchführung, indem Präventionsbedienstete an Schulen entsprechende Zugangslinks zum Online-Fragebogen an Jugendliche verteilen. Die Datenerhebung startete im Schuljahr 2022/23.

Erste Ergebnisse: (1) Verfügbare Zeitressourcen sind sowohl polizeiintern (viele Präventionsbedienstete üben neben der Präventionsarbeit auch andere polizeiliche Tätigkeiten aus) als auch auf schulischer Seite (Aktivitäten während der regulären Unterrichtszeit sind oft nur begrenzt möglich) sehr beschränkt, sodass Präventionsbedienstete Programminhalte oft nur stark verkürzt vermitteln können. (2) Die Anzahl an Anfragen übersteigt häufig die Zahl verfügbarerer Präventionsbediensteter. Um möglichst alle Schulen zu bedienen, finden daher auch aus Effizienzgründen oft stark verkürzte Trainings statt, die zumindest die Grundlagen der präventiven Rechtsinformation vermitteln sollen. (3) Die Abstimmung der Präventionstätigkeit mit sonstigen polizeilichen Verpflichtungen ist herausfordernd, da Kolleginnen und Kollegen aufgrund von Personalmangel fehlende Personalstunden kompensieren müssen und durch das Abwägen der Wertigkeit unterschiedlicher Aufgaben mitunter der Eindruck entsteht, dass der Präventionsarbeit von der Kollegenschaft eine geringere Wertschätzung entgegengebracht wird. (4) In der Praxis werden sehr unterschiedliche Themen an die Präventionsbediensteten herangetragen. Um den spezifischen Bedürfnissen von Schülerinnen, Schülern und Schulen gerecht werden zu können, entstehen daher oft Mischformen der inhaltlichen Gestaltung, die sich nicht ausschließlich den Inhalten eines spezifischen Teilprogramms zuordnen lassen. (5) Manche Präventionsbedienstete – vor allem jene, die ihre Ausbildung Corona-bedingt online absolvieren mussten und praktische Übungen nicht erproben konnten – berichten über pädagogisch-didaktische Unsicherheiten. (6) UNDER18 wird erst seit 2018 österreichweit angeboten, mit Corona-bedingter längerfristiger Unterbrechung. Viele in der Anfangsphase ausgebildete Präventionsbedienstete hatten noch nicht ausreichend Gelegenheit, das Programm entsprechend zu etablieren, was zu Unsicherheiten in der praktischen Umsetzung führt.

Die angeführten strukturellen Probleme äußerten sich im Rücklauf der quantitativen Befragungen der teilnehmenden Schülerinnen und Schüler: Die oft sehr knappen Zeitressourcen erschwerten es den Präventionsbediensteten, zusätzlich Zeit für das Fragebogen-Prozedere (3 Wellen, Experimental- und Kontrollgruppensetting) aufzuwenden. Außerdem zeigten sich Bedenken, ob die Befragungsteilnahme sinnvoll ist, wenn Teilmodule aus den oben genannten Gründen nicht zur Gänze programmkonform abgehalten werden konnten.

Durch intensiven Austausch und Informationsoffensiven werden laufend gemeinsam Lösungen erarbeitet, um die Umsetzung der Präventionstrainings in ihrer Gesamtheit zu erfassen und dabei die strukturellen Herausforderungen und möglichen Unklarheiten zu berücksichtigen: z. B. unterstützende Gesprächs- und Diskussionsrunden, Bereitstellung grafisch unterstützter Ablaufschemata, flexiblere Gestaltung bestimmter Fragebogenelemente. Die Erhebungen unter Schülerinnen und Schülern werden daher noch im Wintersemester 2023/24 fortgesetzt. Erste Ergebnisse aus der ersten Welle der quantitativen Erhebungen, wo die Erwartungshaltung von Schülerinnen und Schülern unmittelbar vor Trainingsbeginn erfasst wurden, bescheinigen den Präventionsbediensteten ein sehr positives und motivierendes Bild: Präventionsbedienstete werden als kompetent, freundlich und verständnisvoll eingestuft, fast 70 % der befragten Schülerinnen und Schüler gaben an, sich bereits auf das bevorstehende Präventionstraining zu freuen.

Projektleitung:

Universität Wien

Projektpartner:

- Bundesministerium für Inneres

Kontakt:

Christiane Atzmüller, Elina Hettich, Assoz. Prof. Dr. Ulrike Zartler, PD
Institut für Soziologie,
Universität Wien
Rooseveltplatz 2
1090 Wien
Tel: +43 1 4277 48244
Mail: ulrike.zartler@univie.ac.at
www.soz.univie.ac.at/ulrike-zartler

FORMA (Forced Marriage)

Lagebericht Zwangsverheiratung in Österreich

Hintergrund

Österreich ist nicht frei vom Phänomen Zwangsheirat, das eine gravierende Menschenrechtsverletzung darstellt; das wahre Ausmaß ist nicht bekannt. Die Kriminalstatistik bildet nur die „Spitze des Eisbergs" ab, da diese Straftat und damit verbundene Problemlagen nach wie vor stark untererfasst sind. Zwangsverheiratung geht oftmals mit Vorbereitungshandlungen außerhalb Österreichs einher und spielt sich zudem im schwer zugänglichen höchstpersönlichen Lebensbereich ab. Des Weiteren erschweren konzeptuelle Abgrenzungsprobleme, etwa zur Aufenthalts- oder Scheinehe und zu ausbeuterischen Formen im Zusammenhang mit Menschen- bzw. Kinderhandel, sowie mangelnde Ursachenforschung sowohl eine effektive Strafverfolgung als auch einen adäquaten Opferschutz. Indem die EU jüngst in ihrem Vorschlag zur Änderung der Richtlinie zur Bekämpfung des Menschenhandels die Zwangsheirat als Ausbeutungsform explizit aufzählt, trägt sie den schweren Eingriffen in die Freiheit und die sexuelle Selbstbestimmung Rechnung, die typischerweise mit diesem Verbrechen einhergehen.

Aufbau der Studie

Ausgehend von der aktuellen österreichischen und internationalen Rechtslage, einschließlich Judikatur und einschlägiger menschenrechtlicher Standards, nimmt das Projekt zunächst eine grundsätzliche Begriffsschärfung und konzeptuelle Abgrenzungen vor. Daran knüpft eine multidimensionale Ursachenanalyse als Basis für die Erarbeitung von Risikoprofilen an, sowie die Analyse, welche Daten für die Identifikation von Problemlagen insbesondere aufseiten potenzieller Opfer benötigt und wie solche Daten erhoben werden könnten. Schließlich werden Vorschläge für präventives Handeln in potenziellen Risikolagen entwickelt.

Um das Ausmaß möglichst umfassend und realistisch zu erfassen, wird anhand verschiedener Fallkonstellationen versucht, alle Formen von Zwangsverheiratungen aufzuzeigen. Welche Aspekte und Ursachen spielen eine Rolle, worin liegen Unterschiede und Gemeinsamkeiten, was bedeutet überhaupt „Zwang"? Kann es sich um Umgehungsformen von Aufenthaltsbestimmungen durch eine Person handeln, wenn diese Opfer von Zwang und/oder Ausbeutung, vielleicht sogar von Menschenhandel geworden ist? Welche Rolle spielen Familienstrukturen, Perspektiven- bzw. Bildungslosigkeit, ökonomische und soziale Abhängigkeiten? In diesem Sinn versteht sich das Projekt auch als Beitrag zu evidenzbasierter Migrationspolitik und allgemein zu Migrationsforschung in Österreich.

Einen eigenständigen Fokus wird das Projekt auch auf die Situation von Kindern und Jugendlichen im Hinblick auf „Kinderehen" bzw. Früh- und Zwangsverheiratungen richten. Als genderbasierte Gewaltform

richtet sich Früh- und Zwangsheirat vordergründig gegen Mädchen, aber keineswegs ausschließlich. Jedenfalls müssen in diesem Kontext Genderaspekte (und damit einhergehend auch die Rolle von Männern und Burschen) in der Ursachenanalyse miteinbezogen werden.

Herausforderungen

Eine besondere Herausforderung des Projekts liegt in der Auseinandersetzung mit „Zwang". Welche Einschränkungen der Handlungsautonomie sind hier relevant, müssen sie explizit sein oder reicht schon impliziter Zwang? Braucht eine Ehe einen klaren Gegenwillen, um als Zwangsehe zu gelten? Inwiefern muss dieser Gegenwille für das Umfeld erkennbar sein, was sagt eine vermeintliche Zustimmung aus? Im Migrationskontext verschärft sich diese Auseinandersetzung, wenn Frauen und Mädchen zur Flucht und gegebenenfalls auch zu einer Ehe gezwungen werden, um an einen vermeintlich sicheren Ort zu gelangen. Fallen diese Betroffenen in den Schutzbereich des rechtlichen Begriffs Zwangsehe?
Zum Zweck einer multidimensionalen Standortbestimmung wird einerseits Feldforschung in Form von qualitativen Interviews mit relevanten Stakeholdern (Sicherheitsbereich/Strafverfolgung, Behörden und Gerichte, Opferschutzeinrichtungen etc.) eingesetzt, andererseits erfolgt eine breit gefächerte Analyse der verfügbaren quantitativen Datenlage.

Ein interdisziplinäres Projektteam, das sowohl rechtswissenschaftliche als auch praktische Erfahrungen mit direkt Betroffenen einbringt, gewährleistet, dass Forschung und Praxis zielorientiert verknüpft, Trends und zukünftige Herausforderungen herausgearbeitet und Handlungsmöglichkeiten für staatliche Akteure, Opferschutzeinrichtungen und für Betroffene selbst signifikant erweitert werden können. Die Laufzeit der Studie ist von Jänner 2023 bis Ende Juni 2024.

Projektleitung:

Caritas der Erzdiözese Wien

Projektpartner:

- Verein Orient Express – Beratungs-, Bildungs- und Kulturinitiative für Frauen
- Ludwig Boltzmann Institut für Grund- und Menschenrechte
- Universität Wien, Institut für Strafrecht und Kriminologie
- Bundesministerium für Inneres
- Bundeskanzleramt – Frauensektion

Kontakt:

Maryam Alemi, M.A, B.A
Caritas der Caritas der Erzdiözese Wien – Hilfe in Not
Mariannengasse 11
1090 Wien
Tel: +43 676 676 6461
Mail: maryam.alemi@caritas-wien.at
www.caritas-wien.at

FRALTERNA

Evaluation der Anwendungspraxis von Freiheitsbeschränkungen und alternativer Maßnahmen bei Gefährdungslagen in Heimen

Ausgangslage, Problematik und Motivation

Freiheitsbeschränkungen in Pflege- und Betreuungseinrichtungen für Menschen mit Behinderungen oder psychischer Erkrankung zur Abwehr einer Selbst- oder Fremdgefährdung stellen als Maßnahmen staatlicher Zwangsgewalt gravierende Eingriffe in die Grund- und Menschenrechte dar. Seit 2005 regelt und beschränkt das Heimaufenthaltsgesetz (HeimAufG) in institutionellen Wohn- und Betreuungsformen solche Eingriffe und erklärt deren Reduktion auf ein möglichst niedriges Ausmaß zum Ziel.
Aktuelle Daten zeigen, dass eine beachtliche Anzahl von Personen von Freiheitsbeschränkungen gemäß HeimAufG betroffen ist. Wissenschaftliche Studien über das Ein- und Zusammenwirken von u. a. rechtlichen, institutionellen/organisationalen, fachlichen, sozioökonomischen und kulturellen Faktoren liegen für Österreich nur ungenügend vor.

Forschungsinteressen und Fokussierungen

Die Studie FRALTERNA greift dieses Forschungsdesiderat auf und generiert evidenzbasierte Erkenntnisse, wie unter den spezifischen Rahmenbedingungen des HeimAufG Freiheitsbeschränkungen in unterschiedlichen Heimtypen zum Einsatz kommen, durch die vorgesehenen Instrumente des Rechtsschutzes (v. a. Bewohnervertretung, Gerichte) überprüft und im Pflege- und Unterstützungsalltag durch schonendere Alternativen reduziert werden. Insbesondere außerrechtliche Faktoren, die für die Effekte des HeimAufG von essenzieller Bedeutung sind, werden in den Blick genommen. Die Ergebnisse sollen zum bestmöglichen Schutz der betroffenen Personen vor unzulässiger Freiheitsbeschränkung unter Sicherung der Abwehr ernstlicher und erheblicher Gefährdungen beitragen. Einrichtungen werden bei der Umsetzung hoher Standards und Kontrollorgane in der evidenzbasierten Weiterentwicklung ihrer Vertretungs- und Prüftätigkeit unterstützt.

Methodisches Vorgehen

Die Studie realisierte einen multiperspektivischen und methodenpluralen Forschungszugang samt vertiefender Fallstudien. Ein Zusatzmodul zu Einrichtungen zur Pflege und Erziehung Minderjähriger evaluiert die Anwendung und Akzeptanz des dort seit 2018 geltenden Gesetzes sowie zielgruppenspezifische Herausforderungen.

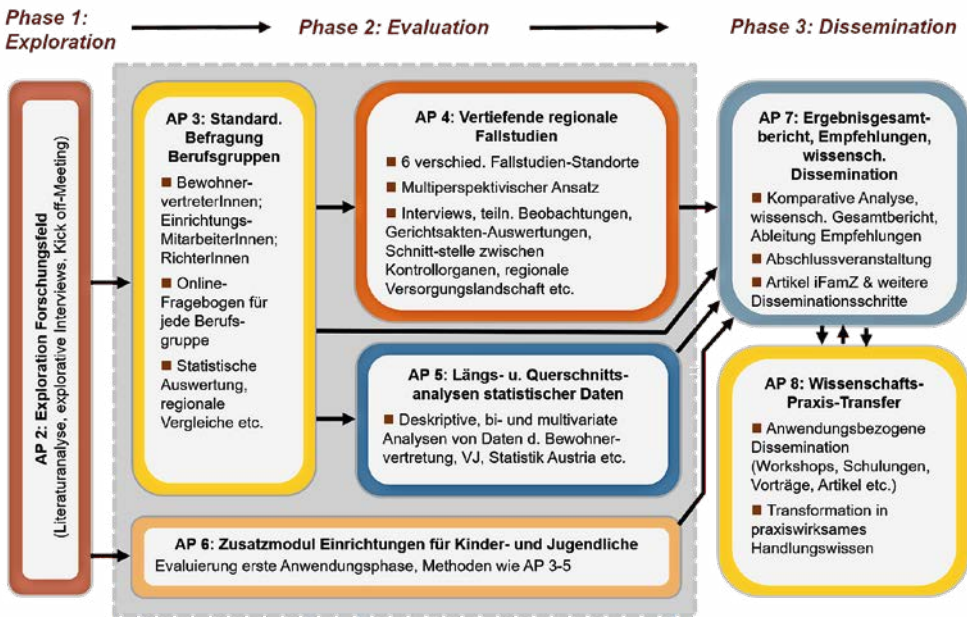


Abb.: Projektaufbau und Forschungsdesign FRALTERNA

Ergebnisse

1. Einstellungen zum HeimAufG und zu Freiheitsbeschränkungen: Die Ergebnisse verdeutlichen, wie Haltungen und Einstellungen relevanter Berufsgruppen mit der Anwendungspraxis von Freiheitsbeschränkungen und Alternativen, aber auch der Überprüfungspraxis in Verbindung stehen.
2. Einsatzpraxis von Freiheitsbeschränkungen und einwirkende Faktoren: Das Ausmaß an Freiheitsbeschränkungen, Strukturen und Prozesse, die darauf einwirken, Gründe für Beschränkungen oder Veränderungen der Anwendungspraxis im Laufe der Zeit wurden umfassend untersucht. Über multivariate lineare Regressionsanalysen konnten zudem Faktoren identifiziert werden, die das Ausmaß an Freiheitsbeschränkungen signifikant beeinflussen. Auf dieser Basis ließen sich Herausforderungen und Ansatzpunkte für Verbesserungen identifizieren.
3. Überprüfungstätigkeit der Bewohnervertretung und Gerichte: Ein Schwerpunkt der Studie liegt auch auf der Erforschung der Überprüfungspraxis durch die Vereine für Bewohnervertretung und das Zusammenwirken von Bewohnervertretung und Einrichtungen bei der Überprüfung von Freiheitsbeschränkungen. Die Umsetzung der gerichtlichen Überprüfung von Beschränkungsmaßnahmen ermöglicht zusätzliche Erkenntnisse zur Rechtsanwendung. Die Studienergebnisse zeigen sowohl große Erfolge als auch einige Herausforderungen auf und können Lernprozesse anstoßen.
4. Effekte des Heimaufenthaltsgesetzes: Die quantitative und qualitative Erfassung von Wirkungen des seit 2005 bzw. 2018 (Minderjährige) geltenden HeimAufG trägt zur Gesamtbewertung der damit geschaffenen Rechtsschutzinstrumente bei.

Projektleitung:

Institut für angewandte Rechts- und Kriminalsoziologie, Universität Innsbruck

Projektpartner:

- Bundesministerium für Justiz
- Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
- Erwachsenenvertretung Salzburg
- Lebenswelt Heim – Bundesverband
- NÖ Landesverein für Erwachsenenschutz (NÖLV)
- VertretungsNetz
- über LoI eingebunden: Institut für Sozialdienste – Bewohnervertretung (Vbg.); Volksanwaltschaft

Kontakt:

Ass.-Prof. Dr. Hemma Mayrhofer
Institut für angewandte Rechts- und Kriminalsoziologie, Universität Innsbruck
Museumstraße 5/12
1070 Wien
Tel: +43 512 507 73900
E-Mail: hemma.mayrhofer@uibk.ac.at
www.uibk.ac.at/irks/

gAia – Predicting landslides

Entwicklung von Gefahrenhinweiskarten für Hangrutschungen aus konsolidierten Inventardaten

Es gilt als wissenschaftlicher Konsens, dass der Klimawandel zu einer Zunahme extremer Wetterereignisse auf globaler Ebene führt, wobei die europäischen Alpen überproportional stark betroffen sind (IPCC, 2021). Änderungen in Niederschlagsmustern können dabei zu einem häufigeren Auftreten gravitativer Massenbewegungen wie Hangrutschungen führen (Offenthaler, 2020; Maraun, et al., 2022). Da gravitative Naturgefahren ein Sicherheitsrisiko für die Gesellschaft darstellen und umfangreiche Schäden an der Infrastruktur verursachen können, sind zuverlässige Methoden zur Vorhersage der Eintrittswahrscheinlichkeit solcher Ereignisse für proaktives Risikomanagement von entscheidender Bedeutung. Ein qualitativ hochwertiges und möglichst vollständiges Ereignisinventar ist eine wesentliche Voraussetzung für ein besseres Verständnis von Hangrutschungen und für die Erstellung von Gefahrenhinweiskarten sowie für Entscheidungen im Katastrophenmanagement. Ereignisdaten für Hangrutschungen stammen aus verschiedenen Quellen, wie historischen Archiven, Feldkartierungen oder Fernerkundungsdaten. Es fehlt jedoch ein ganzheitlicher Ansatz, bei dem qualitative und multimodale Aspekte der Datenfusion berücksichtigt werden.

Das gAia-Projekt hat es sich zum Ziel gesetzt, bestehende Inventare durch den Einsatz von maschinellen Lernverfahren zu ergänzen. Der Schwerpunkt liegt hierbei auf der Detektion von seichtgründigen Hangrutschungen sowie auf der Erstellung von interpretierbaren Gefahrenhinweiskarten für solche Ereignisse.

In einer Fokusgruppe mit wichtigen Stakeholdern, die an der Nutzung der aus dem Projekt resultierenden Gefahrenhinweiskarte interessiert sind, wurde primär die unzureichende Datenqualität als Hauptursache für die mitunter erheblichen Unsicherheiten bei der Modellierung der Eintrittswahrscheinlichkeit solcher Ereignisse identifiziert. Außerdem wurde der Visualisierung der Ergebnisse eine zentrale Bedeutung zugemessen, speziell in Bezug auf eine zielgruppengerechte Aufbereitung.

Im Rahmen von gAia werden verschiedene Methoden des maschinellen Lernens angewendet, um (i) multiple Datenmodalitäten zu fusionieren, (ii) Hangrutschungen anhand von Satellitendaten zu erkennen, (iii) die Auftretenswahrscheinlichkeit von Hangrutschungen zu modellieren und (iv) die Qualität und Erklärbarkeit zu sichern.

Die Detektion von Hangrutschungen auf Basis von Satellitenbildern erfolgt durch die Erkennung von temporalen Veränderungen (change detection) eines Vegtationsindexes (Normalized Difference Vegetation Index; NDVI).

Um Fehldetektionen durch andere Faktoren, welche Veränderungen im NDVI hervorrufen können (z. B. kleinräumige Bautätigkeiten, Holzfällungen, Windwurf etc.), zu minimieren, werden Randbedingungen über weitere Datenquellen (z. B. Wetterdaten) spezifiziert.
Ein weiterer innovativer Aspekt des Projekts ist die Auswertung von Pixel-Nachbarschaftsinformationen (Im & Jensen, 2005) als zusätzliches Merkmal für den Change-detection-Algorithmus. Dadurch können kleinräumige Veränderungen leichter ausgeschlossen werden.
Die finalen Gefahrenhinweiskarten werden schließlich auf Basis des aktualisierten, konsolidierten Inventars erstellt. Dabei wird eine Vielzahl an unabhängigen Variablen aus den Bereichen Morphometrie und Hydrologie, Geologie und Bodenkunde (geotechnische Eigenschaften), Landbedeckung und Klimatologie herangezogen, die in einem Expertenworkshop auf ihre Relevanz für gravitative Hangrutschungen hin definiert und evaluiert wurden.
Um möglichst robuste Aussagen tätigen zu können, wird zudem ein Ensemble an nichtparametrischen Modellen erstellt, welche jeweils unter Berücksichtigung der räumlichen Autokorrelation validiert werden, und auf die Visualisierung der so ermittelten Unsicherheiten Wert gelegt. Auf diese Weise erhalten Stakeholder auf ihre Bedürfnisse angepasste Gefahrenhinweiskarten zur verbesserten Evaluierung der Eintrittswahrscheinlichkeit von seichtgründigen Hangrutschungen. Das Ziel ist es, durch die Erstellung von Gefahrenhinweiskarten potenziell risikobehaftete Gebiete zu erkennen und dadurch die Planung von Präventionsmaßnahmen zu verbessern.

Das Projekt gAia wird im Rahmen des Österreichischen Sicherheitsforschungsprogramms von der Österreichischen Forschungsförderungsgesellschaft (FFG) unter dem Förderungsvertrag FO999886369 gefördert.

Projektleitung:

SBA Research gGmbH

Projektpartner:

- AIT Austrian Institute of Technology GmbH
- Bundesministerium für Landesverteidigung
- Disaster Competence Network Austria - Kompetenznetzwerk für Katastrophenprävention
- Geologische Bundesanstalt
- GeoVille Informationssysteme und Datenverarbeitung GmbH
- Zentralanstalt für Meteorologie und Geodynamik

Kontakt:

Mag. DI Rudolf Mayer
SBA Research gGmbH
Floragasse 7/5
1040 Wien
Tel: 43 1 505 36 88
E-Mail: rmayer@sba-research.org
www.sba-research.org/

GNSS-Check

GNSS-Risikoeinschätzungstool

Im Forschungsprojekt GNSS-Check soll ein Tool entwickelt werden, das Nutzer von satellitenbasierter Navigations-, Positions- und Zeitinformation (ohne dazugehöriges spezifisches Wissen) dabei unterstützt, die Verwendung von Globalen Navigationssatellitensystem (GNSS)-Services in ihren Anwendungen zu verstehen und das damit assoziierte Risiko hinsichtlich Störeinflüssen einschätzen zu können. Im Rahmen des Projekts soll untersucht werden, wie österreichische Stakeholder die Auswirkungen des GNSS-Verlusts auf Anwendungen, Applikationen sowie Organisationen im Bereich der nationalen kritischen Infrastruktur quantifizieren können, und basierend darauf sollen Maßnahmen für ihren operativen Betrieb abgeleitet werden.

Bereits 2014, im Rahmen der Krim-Krise, wurden massive GNSS-Störattacken detektiert und dokumentiert, mit Auswirkung auf die dortige kritische Infrastruktur (z. B. Flughafen – Ausfall GBAS, Mobilfunkunternehmen – Ausfall der Zeitsynchronisierung). In den vergangenen Jahren hat die Zahl solcher Vorfälle global gesehen dramatisch zugenommen und es ist davon auszugehen, dass es in Zukunft auch in Österreich zu weiteren Vorfällen kommen wird. Die kritische Infrastruktur stellt einen besonders sensiblen Bereich des österreichischen Staates dar.

GNSS-Technologien und -Anwendungen werden immer wichtiger und beeinflussen mittlerweile große Teile des täglichen Lebens. Oft wird übersehen, dass viele unserer täglichen Aktivitäten direkt oder zumindest indirekt von GNSS-Services abhängen. Eine der größten indirekten Abhängigkeiten entsteht dadurch, dass sich viele industrielle Stakeholder, Anwendungen und Betreiber kritischer Infrastruktur (zumindest teilweise) auf GNSS verlassen. Aufgrund der Tatsache, dass Signalinterferenzen und andere störende Events durch die technischen Möglichkeiten und die gesteigerte Nutzung zunehmen werden, wird sich auch das Gefahrenpotenzial erhöhen.

Daher ist es unvermeidlich, nun Maßnahmen zu ergreifen, um GNSS-Benutzer, insbesondere die der kritischen Infrastruktur, in Zukunft besser schützen zu können. Insbesondere wird der Sicherheitskultur in Bezug auf die Verwendung von GNSS im Zusammenhang mit intentionalen Gefahren in Organisationen der kritischen Infrastruktur wenig Beachtung geschenkt.

Im Rahmen eines GNSS-Risikomonitorings ist es nicht nur wichtig, Bedrohungen zu detektieren und zu klassifizieren, sondern auch die Identifizierung und Analyse unterschiedlicher Bedrohungsszenarien vor dem Einsatz der Anwendung, Strategien zur Risikominimierung und deren Erfolgschancen zu beachten.

In GNSS-Check werden daher Sicherheitskultur in Organisationen der kritischen Infrastruktur mit dem Fokus auf Gefahren für GNSS-Anwendungen erhoben und analysiert. GNSS-Nutzerinnen und -Nutzer werden dabei unterstützt, die Verwendung von GNSS-Services in ihren Anwendungen zu verstehen, um das damit assoziierte Risiko einschätzen zu können.

In GNSS-Check soll ein Tool entwickelt werden, das Nutzerinnen und Nutzer von satellitenbasierter Navigation, Positions- und Zeitbestimmung dabei unterstützt, die Verwendung von GNSS-Services in ihren Anwendungen zu verstehen und das damit assoziierte Risiko einschätzen zu können. Das Forschungsvorhaben soll eine systematische Bewertung der Risiken durch Verlust oder Abfall von GNSS-Signalen, -Diensten oder - Anwendungen ermöglichen. Basierend auf der Risikobewertung, sollen Nutzerempfehlungen (z. B. Verwendung von Augmentierungsdiensten, geänderte Verfahrensweise, andere Sensorik etc.) ausgesprochen werden. Die Ergebnisse sollen auf eine Vielzahl von Nutzern mit unterschiedlichen Bedürfnissen, verschiedenen GNSS-Anwendungen, unterschiedlichen Bedrohungen/ Schadensanfälligkeiten und unterschiedlichen Ebenen der fachlichen Kompetenz anwendbar sein. Es soll so den österreichischen Stakeholdern im Bereich der sicherheitskritischen Infrastruktur ermöglichen, die Abhängigkeit von GNSS zu quantifizieren und die Belastbarkeit auf organisatorischer, industrieller und nationaler Ebene zu analysieren.

Im Rahmen des Projekts sollen die Grundlagen und wissenschaftlichen Problemstellungen gelöst werden, damit im Endausbau den österreichischen Nutzern der kritischen Infrastruktur, den Behörden und weiteren relevanten Stakeholdern ein (Online-)Tool zur Verfügung gestellt werden kann.

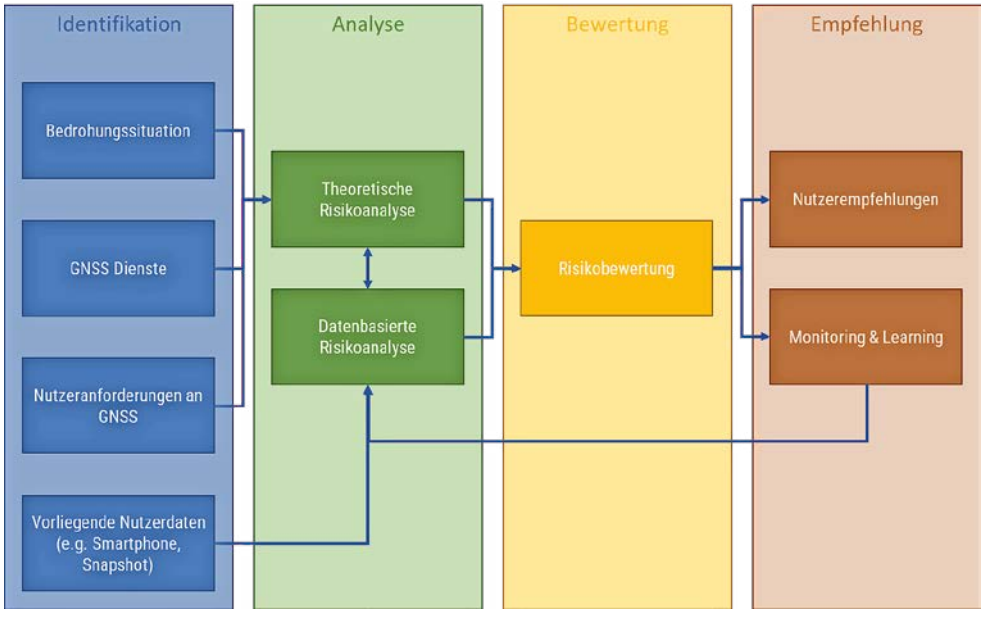


Abb.: GNSS-Check Schema

Projektleitung:

Brimatech Services GmbH

Projektpartner:

- Bundesministerium für Landesverteidigung
- Joanneum Research – Digital, Weltraumtechnik und Kommunikationstechnologie
- Technische Universität Graz – Institut für Geodäsie, Arbeitsgruppe Navigation
- Subcontract: Disaster Competence Network Austria (DCNA)

Kontakt:

Dr. Susanne Katzler-Fuchs
Brimatech Services GmbH
Lothringerstr. 14/3
1030 Wien
Tel: +43 664 968 94 21
E-Mail: skf@brimatech.at
www.brimatech.at

G-Star

Gesamtstaatliche Erfassung der Resilienz im Kontext komplexer Krisenszenarien

Die Bewältigung von komplexen und gleichzeitig auftretenden Bedrohungen wie Epidemien, Blackouts, Cyberangriffen oder Extremwetterereignissen stellt eine Herausforderung dar, bei der effektive Kommunikation und Kooperation aller beteiligten Stakeholder und Akteure von großer Bedeutung sind. Rahmenbedingungen wie begrenzte personelle, finanzielle, immaterielle und materielle Ressourcen haben starken Einfluss auf die Krisenbewältigung. Zusätzlich sind eine effektive Krisenkommunikation und das Vertrauen in die handelnden Akteure wichtige Grundpfeiler für ein effektives und resilientes Krisenmanagement. Das Ziel des Projekts G-Star war die Erfassung der kooperativen Strukturen des österreichischen Krisenmanagements und die Bewertung des Gesamtnetzwerkes in Hinblick auf seine Resilienz. Der Forschungsgegenstand wurde durch die Kombination verschiedener Erhebungs- und Analysemethoden umfassend beleuchtet. Durch Kombination aus Desktop-Recherche, Experteninterviews und der Durchführung von Mixed-Methods-Fokusgruppen sammelten wir Datenmaterial sowohl in der Tiefe als auch der Breite. Die Teilnehmerinnen und Teilnehmer wurden so gewählt, dass verschiedene Positionen im gesamtstaatlichen Netzwerk abgebildet werden konnten. In den Interviews stellten sich eine Pandemie sowie ein Blackout als bedeutungsvolle Bedrohungsszenarien dar, wodurch ein Szenario, das diese beiden Bedrohungen kombinierte, als Grundlage der Diskussion in den Fokusgruppen diente. Das große Interesse und die Teilnahme der Stakeholder und Akteure an dieser Studie unterstreichen die hohe Relevanz der betrachteten Thematik.

Die erhobenen Daten wurden anhand einer Resilienz-Taxonomie und Resilienz-Ontologie, einer graphentheoretischen Modellbildung (Netzwerkanalyse) sowie einer Resilienzanalyse ausgewertet und aufbereitet. Abschließend wurden in Zusammenarbeit mit dem Bundeskanzleramt und dem Bundesministerium für Inneres Handlungsempfehlungen abgeleitet. Unterschiede im Verständnis von Begrifflichkeiten können zu Kommunikationsschwierigkeiten und Missverständnissen in der Krisenbewältigung führen. Das gemeinsame Verständnis und die semantische Interoperabilität sind daher unbedingt notwendig, um Kommunikationsbarrieren zu überwinden und die Zusammenarbeit zu verbessern. Zu diesem Zweck wurde eine Resilienz-Taxonomie und -Ontologie erstellt. Basierend auf den Ergebnissen liegt die Empfehlung darin, das bestehende Normdokument ÖNORM S 2304 um die erarbeiteten Begriffe zu erweitern, um so eine effiziente und eindeutige Kommunikation sicherzustellen.

Die Netzwerkanalyse basierte auf den Erkenntnissen der Experteninterviews sowie Fokusgruppen und stellte eine aktuelle Darstellung der realen Situation dar: Krisensituationen 2 G-Star werden in Österreich

vorrangig auf Gemeinde- bzw. Landesebene koordiniert, wobei dem Bundesministerium für Inneres eine Schlüsselrolle in der Kommunikation auf Bundesebene und dem Informationsaustausch mit außerbehördlichen Organisationen zukommt. Andere Bundesressorts sind weniger stark in die Kommunikation eingebunden, wodurch Silos im Krisen- und Katstrophenmanagement entstehen können. Auf Basis der Analysen des graphentheoretischen Modells lässt sich empfehlen, dass die Kommunikationsmedien in Zukunft tiefer untersucht werden sollten, um die Simulation von Ausfällen gewisser Kommunikationsinfrastrukturen und deren Auswirkungen erheben und bewerten zu können.

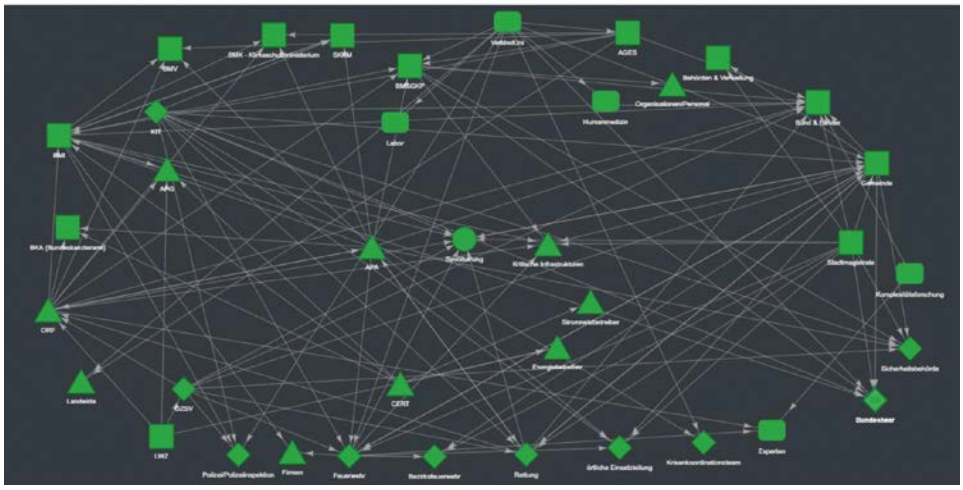


Abb.: Graphentheoretisches Modell mit allen relevanten Stakeholder-Gruppen

Die Herausforderung der Resilienzanalyse lag darin, die Methode der SWOT-Analyse auf eine empirische Studie zu übertragen und die gesammelten Ergebnisse zu strukturieren. Dabei konnten Kategorien gebildet werden, die als Stärken, Schwächen, Chancen und Bedrohungen Einfluss auf die gesamtstaatliche Resilienz des österreichischen Krisen- und Katastrophenmanagements haben. Ein gemeinsames Auftreten, eine umfassende Risikoanalyse oder gesetzliche Anpassungen sowie das Sozialkapital konnten dabei als besondere Stärken und Chancen identifiziert werden. Unklare Kompetenzverteilung, datenschutzrechtliche Silos oder weitreichende Kaskadeneffekte wurden als Schwächen und Bedrohungen der Resilienz angesehen (3 G-Star).

Die G-Star-Studie liefert einen Einblick in das österreichische Krisen- und Katastrophenmanagement und die Perspektiven der zu beachtenden Aspekte. Es konnte ein Kommunikationsnetzwerk erarbeitet werden, wodurch krisenbedingte Ausfälle leichter zu simulieren sind und Maßnahmen getroffen werden können.

Projektleitung:

SBA Research gGmbH

Projektpartner:

- AIT Austrian Institute of Technology GmbH
- Bundeskanzleramt Österreich, Abteilung IV/6: Sicherheitspolitik
- Bundesministerium für Inneres
- Disaster Competence Network Austria - Kompetenznetzwerk für Katastrophenprävention

Kontakt:

Dr. Johanna Ullrich
SBA Research gGmbH
Floragasse 7/5
1040 Wien
Tel: +43 1 505 36 88
E-Mail: jullrich@sba-research.org
www.sba-research.org

HYBRIS

Hybride Bedrohungs-Resilienz durch interdisziplinäre Zusammenarbeit der Sicherheitsbehörden

HYBRIS befasst sich mit hybriden Bedrohungen, welche die Absicht verfolgen, durch online koordinierte Operationen Überzeugungen und Einstellungen ausgewählter Zielgruppen zu beeinflussen, diese zum Handeln zu mobilisieren und in der Folge die physische und digitale Infrastruktur zu kompromittieren. Desinformation ist ein wesentlicher Bestandteil hybrider Bedrohungen. Desinformationskampagnen zielen häufig darauf ab, Ängste in der Bevölkerung zu schüren, die unterschiedliche Folgen nach sich ziehen können. Unabhängig davon, ob es sich bei Nachrichten um Falschinformationen handelt oder nicht, ist es für Sicherheitsbehörden wichtig zu erkennen, ob von Reaktionen auf Nachrichten in sozialen Medien und anderen Nachrichtenkanälen bzw. möglicherweise in der Folge organisierter Aktionen eine Bedrohung für Menschen oder kritische Infrastruktur ausgeht. Im Falle der Verbreitung von Desinformation geht es auch darum, geeignete Maßnahmen zu ergreifen: etwa durch die Erstellung und Verbreitung von auf Tatsachen und vertrauenswürdigen Informationen basierenden Gegendarstellungen einer bedrohlichen Entwicklung entgegenzuwirken.

Besonders wichtig ist es, schnell auf diese Art von Nachrichtentrends zu reagieren. Daher muss die inhaltliche Vorbereitung möglicher Gegendarstellungen bereits beginnen, wenn diese noch im Entstehen sind. Eine der wesentlichen Herausforderungen ist dabei die Gewährleistung eines umfassenden Überblicks (Situational Awareness) über die aktuell vorherrschenden Trends. Die Schwierigkeit dabei ist, dass Informationen über eine unüberschaubare Zahl von Informationskanälen in hoher Geschwindigkeit ausgetauscht werden, und dass es unmöglich ist, sich einen Überblick durch manuelle Sichtung zu verschaffen. Darüber hinaus muss die Vertrauenswürdigkeit der Informationen im Zuge des Abgleichs verschiedener Informationsquellen und Modalitäten, also z. B. Text, Bild oder Ton, eingeschätzt werden. Für diese Aufgaben ist es dringend erforderlich, die Sicherheitsbehörden durch automatisierte und KI-basierte Systeme bei der Informationssichtung und Überblickserstellung zu unterstützen.

Die Herausforderung für Sicherheitsbehörden liegt dabei in der Bewältigung der Informationsflut, welche mit der stetig anwachsenden Datenlast einhergeht.
Ein übergeordnetes Ziel von HYBRIS ist, unstrukturierte Daten mit Hilfe künstlicher Intelligenz so zu strukturieren, dass ein möglichst breiter Überblick über wesentliche Informationen gewährleistet werden kann. Hierfür sollen Ansätze zur Erkennung relevanter Narrative wie „Mutmaßliche Treibstoffknappheit“, welche durch die Auswirkung „Stau vor Tankstellen“ eine Bedrohung für die kritische Infrastruktur „Verkehr“ darstellt, erforscht werden. Durch die Erkennung von Narrativen und deren Kontext erlangen

Sicherheitskräfte den nötigen Handlungsspielraum, um entsprechend darauf reagieren zu können. Nach Themen, Narrativen oder Kategorien strukturierte Inhalte sollen automatisiert z. B. bezüglich Desinformation bewertet werden, damit eine Einteilung hinsichtlich hybrider Bedrohungen möglich ist, was den Entscheidungsspielraum der Behörden zusätzlich erweitert.

HYBRIS soll prototypisch für eine nationale Data-Intelligence-Plattform stehen, anhand derer eine Entscheidungsgrundlage zur Verbesserung der Effektivität und Resilienz der österreichischen Sicherheitsbehörden erstellt wird. Dabei werden bestehende KI-Tools zusammengeführt, die mit automatisiert extrahierten Daten aus Online-Quellen und Social Media potenzielle Gefahren aufzeigen sollen. Zur schnelleren Prozessierung wird auch eine effektive und wenn möglich parallele Prozessierung der Daten untersucht.

In Anbetracht der zu bewältigenden Informationsflut, die mit der Erkennung von hybriden Bedrohungsszenarien verbunden ist, wird im Rahmen von HYBRIS die Recht- und Verhältnismäßigkeit hinsichtlich des zu wahrenden Grund- und Menschenrechtsschutzes umfassend zu berücksichtigen sein. Die Vereinbarkeit mit den rechtlichen Gegebenheiten im Hinblick auf das Datenschutzrecht und zentralen ethischen Gesichtspunkten wird dabei eine gewichtige Rolle spielen. Dahingehend ist als weiterer wesentlicher Aspekt die Erforschung vertrauensbildender Verfahren und Werkzeuge anzuführen, welche den Einsatz von künstlicher Intelligenz in solch einem komplexen Bereich evaluieren und validieren. Hierfür werden mit Ethics by Design und Lawfulness by Design Ansätze verfolgt, welche sicherstellen, dass hier eine ethisch und rechtlich konforme Umsetzung gewährleistet wird.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Research Institute AG & Co KG
- Thinkers.ai
- TU Wien
- Universität für Bodenkultur Wien
- Artificial Researcher IT GmbH
- Bundesministerium für Landesverteidigung

Kontakt:

Dr. Alexander Schindler
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 2902
E-Mail: Alexander.Schindler@ait.ac.at
www.ait.ac.at

IKKRITI

Integrale Konsequenzanalyse für kritische Infrastrukturen

Die rasch fortschreitende Digitalisierung und deren Auswirkungen auf kritische Infrastrukturen stellen hohe Anforderungen an die Sicherheitspolitik und entsprechende Bedarfsträger, da viele Versorgungssysteme untereinander vernetzt sind. Digitale Technologien können dabei sowohl ein großes Risikopotenzial als auch mehr Chancen für die Sicherheit darstellen.

Vor diesem Hintergrund war es **Ziel** dieses Projektes, ein Steuerungsinstrument für Bedarfsträger im sicherheitspolitischen Bereich in Form einer „Integralen Konsequenzanalyse für Kritische Infrastrukturen (IKKRITI)“ zu entwickeln. Dieses soll Entscheidungsträger bei der Strategieentwicklung durch eine aktualisierbare und reproduzierbare Wissensbasis unterstützen, die systematisch die Chancen, Risiken und Herausforderungen technischer und gesellschaftlicher Entwicklungen berücksichtigt und einer transparenten Bewertungslogik folgt.

Mittels Integration von **Methoden** der Foresight und der Technikfolgenabschätzung und eines bereits existierenden Tools zu Technologie- und Trendmonitoring wurden die Auswirkungen digitaler Technologien in Bezug auf kritische Infrastrukturen analysiert, mögliche Zukünfte antizipiert und strategische Handlungsoptionen anhand der Use Cases „eID“ (elektronische Identität) und „WarnApps“ identifiziert. Das **Ergebnis** des Projektes ist ein Steuerungsinstrument, das die unterschiedlichen Perspektiven und Methoden in einem handlungsleitenden Ansatz zusammenführt.

Die acht Elemente (Werkzeuge, Tool-Chain) des Steuerungsmodells sind in Abbildung dargestellt. Begonnen wird mit einer (i) Zielidentifikation (scoping), die im IKKRITI-Steuerungsmodell mit einer Funktionsanalyse realisiert wurde. D. h., es wurden mittels einer Analyse digitaler Bedrohungen im Bereich kritischer Infrastrukturen sicherheitsrelevante Trends sowie die daraus resultierenden Risiken identifiziert. Innerhalb des in der Funktionsanalyse abgegrenzten Untersuchungsbereichs werden vertiefende Analysen vorgenommen, die innerhalb einer Strategieperiode gegebenenfalls zu aktualisieren sind (ii-iv). D. h., es werden Technologiecluster und komplementär dazu Umfeldtrends identifiziert und analysiert, in denen und mit denen die Technologiecluster im realen Rahmen interagieren müssen. Anschließend werden die Top-Cluster & Top-Trends einer Wechselwirkungsanalyse unterzogen. Im Projekt IKKRITI bildeten die höchst priorisierten Cluster & Trends die Basis für die Auswahl der Use Cases „eID“ und „WarnApps“.

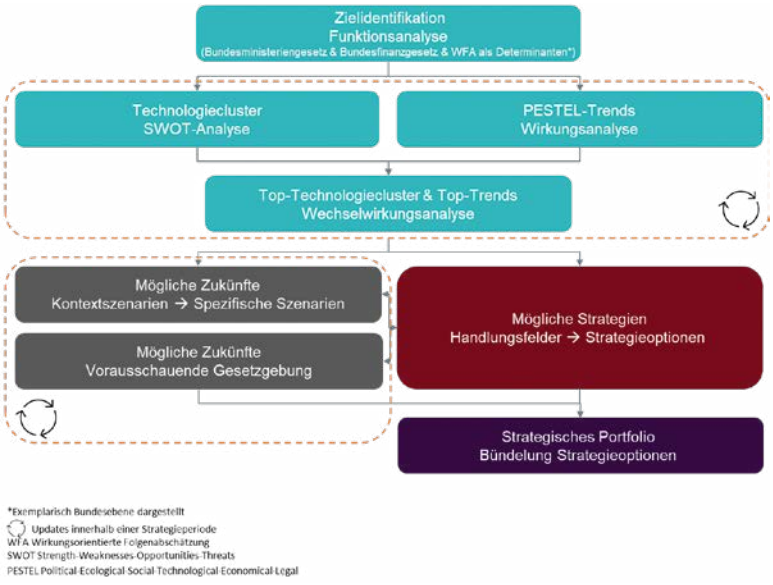


Abb.: Modellelemente (Tool-Chain) der integralen Konsequenzanalyse als Steuerungsinstrument

Wiewohl in die Trend-Analysen bereits Annahmen über zukünftige Entwicklungen einfließen, gehen Zukunftsentwürfe noch darüber hinaus, indem Szenarien nicht nur sich abzeichnende Trends betrachten, sondern assoziativ-kreativ auch Unsicherheiten, Überraschungen, Seltenheiten und mögliches Nichtwissen (Wild Cards, Black Swans, Unknown Unknowns) reflektieren. Daher enthält das IKKRITI-Steuerungsmodell (v) Kontextszenarien und spezifische Digitalisierungsszenarien, die die Erkenntnisse der Trend- & Cluster-Analysen aufnehmen und weiterführen und mittels (vi) vorausschauender Gesetzgebung ergänzt werden. Die beiden abschließenden Elemente sind die (vii) Abgrenzung von Handlungsfeldern und das Überführen von Handlungsoptionen in (viii) Strategieoptionen und ein strategisches Portfolio. Im Projekt IKKRITI wurden die Handlungsfelder in Bezug auf die Use Cases abgegrenzt, anhand derer Handlungs- und Strategieoptionen ausgearbeitet wurden.

Reflexion und Ausblick: Das IKKRITI-Modell repräsentiert die erfolgreiche Pilotanwendung einer integralen Konsequenzanalyse zur Unterstützung von Entscheidungsträgern im sicherheitspolitischen Bereich. Für das Gelingen des IKKRITI-Projektes war die engagierte und unterstützende Mitwirkung der Vertreterinnen und Vertreter der Bedarfsträger über die gesamte Projektlaufzeit von größter Bedeutung. Nach dieser Pilotierung soll das IKKRITI-Modell an weiteren Use Cases im Bereich der kritischen Infrastrukturen erprobt und verbessert werden.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- A-SIT Zentrum für sichere Informationstechnologie Austria
- Bundesministerium für Digitalisierung und Wirtschaftsstandort
- Bundesministerium für Landesverteidigung
- REPUCO Unternehmensberatung GmbH
- SBA Research gemeinnützige GmbH
- TU Technische Universität Wien

Kontakt:

Eva Buchinger
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4543
E-Mail: eva.buchinger@ait.ac.at
www.ait.ac.at

INFRASPEC

Automatische Inspektion von kritischer Infrastruktur

Das KIRAS-Projekt INFRASPEC erforscht neuartige Methoden zur robotergestützten Detektion von Gefahren durch Veränderungen und Leckagen von Gefahrenstoffen in Versorgungsschächten kritischer Infrastruktur sowie die technologische Unterstützung durch eine ferngesteuerte Detailuntersuchung im Alarmfall. Zielsetzung ist die Erhöhung des Schutzes und der Verfügbarkeit kritischer Infrastruktur sowie der Ausbau der Vorreiterrolle in der automatisierten Sicherheitsinspektion.

Kritische Infrastrukturen bilden die Grundlage für die Versorgung der Bevölkerung mit lebensnotwendigen Diensten und Gütern wie Energie, Wasser und Daten. Ein Ausfall oder eine Beeinträchtigung kann zu erheblichen Störungen der öffentlichen Sicherheit führen. Zu diesen Bauwerken gehören ausgedehnte und komplexe Netzwerke von Versorgungsschächten (sog. Kollektorgängen) mit bis zu mehreren Hundert Kilometern Ausdehnung. Diese tragen ein hohes Risiko für Störfälle, können aber auch Ziele für bewusste Manipulationen oder Handlungen mit krimineller Absicht sein. Die schwierigen Umgebungsbedingungen, wie lange Gänge mit geringem Lichtraum oder die eingeschränkte Zugänglichkeit, stellen für das zuständige Personal besondere Herausforderungen bei den vorgeschriebenen regelmäßigen Kontrollen der technischen Betriebszustände (Dichtheit, Wärmeverlust etc.) und der baulichen Substanz dar. Darüber hinaus ist die Vulnerabilität von kritischen Rohr- und Kabelschächten auch im Hinblick auf die terroristische Bedrohung von zentraler Bedeutung. Angriffe auf solche Infrastrukturen können im schlimmsten Fall auch zu Todesfällen in der betroffenen Bevölkerung führen.

Ziel des Projekts ist die Entwicklung eines Robotersystems, das das Sicherheitspersonal bei der Überprüfung von Rohr- und Kabelschächten in kritischen Infrastrukturen bestmöglich unterstützt. Die automatische und zuverlässige Detektion von Gefahren durch Veränderungen, wie zum Beispiel die Erfassung von unbekannten Gegenständen, die Erkennung von Manipulationen oder die Beschädigungen der Bausubstanz, sind wesentliche Projektaspekte. Weiters sollen Gefährdungen durch Leckagen von Gefahrenstoffen rasch und sicher erkannt werden. Beispiele sind industrielle Gase, Treibstoffe oder Kältemittel. Hierzu werden die entsprechenden chemischen Sensoren im Projekt evaluiert und am Roboter integriert. Das Hauptaugenmerk des Projekts liegt auf der Entwicklung von Analysemethoden, die auf der Kombination von Umgebungsmodellen aus dreidimensionaler Erfassung und Gefahrenstoffmesswerten aus chemischen Sensoren beruhen. In den verwinkelten Gängen kommt es auch immer wieder zu Verdeckungen durch Ecken und Nischen. Daher befasst sich INFRASPEC auch mit der Entwicklung von Methoden. Das Gesamtsystem teilt sich in eine mobile Roboterplattform mit einem beweglichen Roboterarm, Sensorik und Recheneinheiten zur ersten Detektion und Berechnung von zeitkritischen Aufgaben sowie

eine Basisstation zur Schad- bzw. Gefahrenanalyse und der anschließenden Aufbereitung der Ergebnisse in einer Visualisierung. Die Roboterplattform ist mit Fern- und Nahfeldsensoren ausgestattet. Die Sensoren zur Umgebungserfassung setzen sich aus einem Laserscansystem und einem chemischen Sensor für die Detektion von Gefahrenstoffen zusammen. Die Sensorik dient einerseits dazu, ein dreidimensionales Modell der Umgebung aufzubauen, und andererseits die Veränderungen in der Umgebung sowie atmosphärische Veränderungen zu messen. Die Nahfeldsensoren umfassen einen Abstandssensor für kurze Distanzen und eine Kamera zur visuellen Inspektion. Diese Sensoren sind am Roboterarm angebracht, bewegen sich mit diesem mit und können mit diesem exakt ausgerichtet werden.

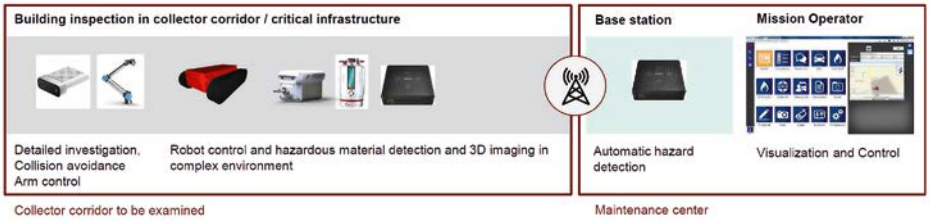


Abb.: Robotersystem zur Inspektion von Rohr- und Kabelschächten

Die INFRASPEC-Projektpartner bilden ein hervorragendes Konsortium für die Entwicklung einer innovativen, bedarfsgerechten Lösung für die robotergestützte Inspektion von kritischen Infrastrukturen und stellen einen vielseitigen Verbund zwischen privatwirtschaftlichen Unternehmen, Forschungseinrichtungen und Bedarfsträgern dar. Die wissenschaftlichen Partner das AIT Austrian Institute of Technology GmbH und die Johannes Kepler Universität Linz JKU entwickeln Methoden und Algorithmen und planen deren Lizensierung für eine spätere Produktumsetzung. Die Bedarfsträger – die Bundesministerien für Inneres (BMI) und für Landesverteidigung (BMLV), die Flughafen Wien AG und die Wiener Netze GmbH – erlangen durch ihre Partizipation an der Forschung und Entwicklung im Projekt einen Know-how-Vorsprung bei der Absicherung und Überwachung ihrer technischen Infrastruktur. Das Disaster Competence Network Austria (DCNA) übernimmt die Risikoanalyse und organisiert eine Table-Top-Exercise, um zentrale Faktoren der Gefahrenwahrnehmung im Zusammenhang mit dem Robotiksystem zu erheben. Die Unternehmenspartner CBRN Protection GmbH und Rosenbauer International AG erweitern im Projekt ihre Erkenntnisse im Bereich der Sensorik, der roboterbasierten Erfassung komplexer Umgebungen und der Interaktion des Laserscanners mit einer mobilen Plattform. Sie sind in der Lage, durch die Ergebnisse dieses Projekts ihre technologische Wettbewerbsfähigkeit zu erhöhen und dadurch neue Geschäftsfelder zu erschließen. Rosenbauer hat zudem durch seine Rolle als Technologieträger und Systemintegrator mit einem weltweiten Vertriebsnetz optimale Voraussetzungen für die Verwertung eines zukünftigen Gesamtsystems für die robotergestützte Inspektion kritischer Infrastruktur.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung
- CBRN Protection GmbH
- Disaster Competence Network Austria
- Flughafen Wien AG
- Johannes Kepler Universität Linz – Institute of Networks and Security
- Rosenbauer International AG
- Wiener Netze GmbH

Kontakt:

DI Michael Hofstätter
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 664 2351858
E-Mail: Michael.Hofstaetter@ait.ac.at
www.ait.ac.at

ISIDOR

Folgen einer langandauernden und großflächigen Einschränkung der internet-basierten Dienste und Infrastrukturen

Das Forschungsprojekt ISIDOR beschäftigte sich mit der Frage, was passiert, wenn das Internet in Österreich großflächig und für einen längeren Zeitraum ausfällt. Dem „All Hazards"-Ansatz des Austrian Programme for Critical Infrastructure Protection (APCIP) folgend, standen nicht die Ursachen eines derartigen Ausfalls und deren Vermeidung im Fokus des Projekts, sondern das Augenmerk wurde auf den Bereich Cyber-Resilience gerichtet. Dabei galt es herauszufinden, wie sich die Lage nach einem Schadensfall entwickeln und wie die dadurch ausgelöste Krise bestmöglich gelöst werden könnte.

Große Schwierigkeiten sind dort zu befürchten, wo IT-Prozesse und -Ressourcen im Normalbetrieb ausgelagert wurden. Das ist beispielsweise bei der Nutzung von Clouddiensten oder dem Outsourcing von IT-Personal der Fall. Ähnlich verhält es sich mit dezentralen mobilen IT-Systemen, wie bspw. der Patientendokumentation im Rettungswesen. Stark betroffen wäre auch der Banken- und Finanzsektor, wo viele Geschäftsprozesse ohne die Möglichkeit zur Datenkommunikation mittlerweile undenkbar sind.

Ein sektorübergreifendes Problem ergäbe sich aus der Betroffenheit des Transportwesens. Ohne Schnittstellen zur Datenkommunikation wäre der Transport von Gütern nur mit Einschränkungen möglich. Die Daten- und Dokumentationsverarbeitung sowie das Transportmanagement (z. B. Sendungsverfolgung, Aviso, Einlagerung, Wiederauffinden, Zustellung etc.) sind in hohem Maße von miteinander vernetzten IT-Systemen abhängig. Gleichzeitig verlassen sich viele Organisationen darauf, dass z. T. mehrmals täglich – just in time – zugestellt wird, um kein großes Lager mit differenziertem Bestand betreiben zu müssen.

Durch die zu erwartenden Einschränkungen in der Mobilkommunikation, entweder durch Ausfall oder Überlastung des Mobilfunknetzes, ist davon auszugehen, dass oftmals Sicherheitstechnik nicht funktionieren wird: Alarmanlagen und Brandmelder, die direkt an Polizei oder Feuerwehr melden, wären ebenso wenig funktionsfähig wie Alarmierungen (z. B. von Krisenstäben) über Apps oder SMS.

Manches davon kann durch die Umstellung auf analoge Prozesse und erhöhten Personaleinsatz ausgeglichen werden, wenn das zuvor geübt wurde und die notwendigen Ressourcen im Krisenfall zur Verfügung stehen.

Der Trend zu Konvergenz in der Infrastruktur und Effizienz in den Geschäftsprozessen führte in den vergangenen Jahrzehnten zu einer starken Reduktion von Puffern im Gesamtsystem. Dadurch steigt nicht

nur allgemein die Abhängigkeit durch die voranschreitende Vernetzung, sondern es sinkt zugleich die Fehlertoleranz des Systems.

Durch die gegenseitigen Abhängigkeiten über sektorale Grenzen hinweg wird es kaum einen Bereich geben, der durch einen Ausfall internetbasierter Dienste nicht beeinträchtigt wäre. Ähnlich wie bei einem großflächigen Stromausfall spricht man auch hier von einer sogenannten vernetzten Krise. Letztendlich ist es auch mit viel Aufwand nicht möglich, genau vorherzusagen, wie die Lage nach so einem Schadensfall aussähe. Zielführender ist es, die Kräfte für das Krisenmanagement zu stärken und die First Responders in Trainings auf eine solche Situation vorzubereiten. Dadurch ließe sich die Handlungsfähigkeit im Ernstfall besser erhalten oder sogar erhöhen.

Mehr Informationen zu den Ergebnissen und Handlungsempfehlungen aus dem Projekt finden Sie in der ISIDOR-Studie (downloadbar unter: https://short.boku.ac.at/isidor).

Projektleitung:

Universität für Bodenkultur Wien – Institut für Produktionswirtschaft und Logistik

Projektpartner:

- Bundesministerium für Digitalisierung und Wirtschaftsstandort (Bedarfsträger)
- Bundesministerium für Inneres (Bedarfsträger)
- Infraprotect Gesellschaft für Risikoanalyse, Notfall- und Krisenmanagement GmbH
- Mar Adentro e.U.
- Österreichische Akademie der Wissenschaften – Institut für Technikfolgen-Abschätzung
- REPUCO Unternehmensberatung GmbH

Kontakt:

Univ. Prof. Dr. Manfred Gronalt
Universität für Bodenkultur Wien – Institut für Produktionswirtschaft und Logistik
Feistmantelstraße 4
1180 Wien
Tel: +43 1 47654 73200
E-Mail: manfred.gronalt@boku.ac.at
www.wiso.boku.ac.at/pwl.html

JUGHENT

Empirische Forschung für die Verortung und Weiterentwicklung der Jugendgerichtshilfe

Repressive strafrechtliche Sanktionen gegen junge Menschen haben oft kontraproduktive Auswirkungen. Die meisten Rechtssysteme sehen daher Möglichkeiten vor, auf Jugenddelikte mit minimaler Intervention, erzieherischen Sanktionen oder sozialkonstruktiv-wiedergutmachenden Maßnahmen zu reagieren. Die Wahl einer angemessenen Reaktionsform setzt Wissen u. a. zu Persönlichkeit und Lebenslage der Beschuldigten voraus. Eine individuelle Begutachtung der Lebensumstände und Hintergründe von straffällig gewordenen Jugendlichen und die Berücksichtigung dieser Informationen aus dem Blickwinkel des Kindeswohls in Verfahren und Entscheidungen sind auch durch internationales, supranationales sowie nationales Recht geboten. Artikel 3 der UN-Konvention über die Rechte des Kindes fordert grundlegend, dass bei „allen Maßnahmen, die Kinder betreffen, gleichviel ob sie von öffentlichen oder privaten Einrichtungen der sozialen Fürsorge, Gerichten, Verwaltungsbehörden oder Gesetzgebungsorganen getroffen werden", das Wohl des Kindes vorrangig zu berücksichtigen ist. In Konkretisierung dieses Artikels sehen die Mindeststandards für die Jugendgerichtsbarkeit der Vereinten Nationen unter anderem vor, dass „der Hintergrund und die Umstände, in denen der Jugendliche lebt oder unter welchen Bedingungen die Straftat begangen wurde, ordnungsgemäß untersucht werden, um der zuständigen Behörde eine sachgerechte Beurteilung des Falles zu erleichtern". Die zuständigen Behörden sollten „über relevante Fakten über den Jugendlichen informiert werden, wie z. B. sozialer und familiärer Hintergrund, Schullaufbahn, Bildungserfahrungen usw." Die Regel verlange, „dass angemessene soziale Dienste zur Verfügung stehen, die taugliche Berichte über Sozialerhebungen erstellen können. Artikel 7 der EU-Richtlinie 2016/800 über Verfahrensgarantien in Strafverfahren für Kinder, die Verdächtige oder beschuldigte Personen in Strafverfahren sind, statuiert ein Recht auf individuelle Begutachtung. Die Mitgliedsstaaten sind verpflichtet sicherzustellen, „dass die besonderen Bedürfnisse von Kindern in Bezug auf Schutz, Erziehung, Ausbildung und soziale Integration" auf der Basis solcher Begutachtungen berücksichtigt werden.

In Österreich ist das Tätigwerden einer Gerichtshilfe in Strafverfahren gegen Jugendliche und junge Erwachsene gesetzlich standardmäßig vorgesehen und damit auch praktisch von enormer Bedeutung. Sie unterstützt Staatsanwältinnen/Staatsanwälte und Richterinnen/Richter bei der Sammlung der erforderlichen psychosozialen Informationen.

Blickt die Wiener Jugendgerichtshilfe auf eine mehr als 110-jährige Tradition zurück, existiert eine österreichweite Jugendgerichtshilfe erst seit 2016. Seit 2020 sind die Erhebungen zu Persönlichkeit und Lebenslage der jugendlichen Beschuldigten bei allen Strafverfahren, wo es zur Anklage kommt,

verpflichtend. Ausnahmen bestehen lediglich in Verfahren, wo ein diversionelles Vorgehen in Aussicht gestellt wird. Die Beauftragung von Erhebungen ist jedoch auch in solchen Verfahren möglich. Die Aufgaben der Jugendgerichtshilfe umfassen das Sammeln von Daten zu Lebenslage und Persönlichkeit beschuldigter Jugendlicher, die Mitwirkung an einem Tatausgleich oder an der Vermittlung gemeinnütziger Leistungen, das Beseitigen bestehender Schäden oder Gefahren für die Erziehung und Gesundheit (Krisenintervention) sowie das Erheben maßgeblicher Umstände zur Entscheidung über Freilassungen und die Äußerung zur Zweckmäßigkeit einer Untersuchungshaftkonferenz bzw. die Teilnahme an solchen. Die Wiener Jugendgerichtshilfe kann zusätzlich auch mit der Betreuung von Untersuchungs- und Strafgefangenen betraut werden.

Trotz der Ausweitung des Anwendungsbereichs und ihrer praktischen Bedeutung fehlen bisher österreichweite empirische Studien zu Nutzung, Arbeitsweise und den Wirkungen der Jugendgerichtshilfe. Im Rahmen von JUGHENT wird die Jugendgerichtshilfe hinsichtlich der Zuweisungspraxis, der Umsetzung ihrer Aufträge sowie deren Wirkungen auf den Ausgang der Verfahren sowie ihre Klientinnen und Klienten untersucht.
Die Komplexität des Forschungsvorhabens erfordert einen kreativen, methodisch breiten Zugang. Es werden sowohl quantitative Daten erhoben als auch qualitative Forschungsmethoden eingesetzt und die so gewonnenen Daten miteinander kombiniert. Dabei vermitteln die aus den vorhandenen Dokumentationen nutzbaren quantitativen Daten eine umfassende Grobstruktur, die durch eine im Rahmen des Projektes geplante Klienten/Klientinnen-Befragung ergänzt wird. Die qualitativen Studien anhand von Akten und Interviews mit Jugendgerichtshelferinnen und -helfern, Richterinnen und Richtern sowie Staatsanwältinnen und Staatsanwälten sowie anderen im Feld relevanten Akteuren ermöglichen wiederum vertiefende Einsichten in Zuweisungsmotive, Fallbearbeitung, in relevante strukturelle Aspekte, qualitative Aspekte der Leistungen der Jugendgerichtshilfe und deren Verwertung bzw. Wirkungen. Schließlich soll das Lernpotenzial von Blicken in andere Länder genutzt werden.

Die Untersuchungsergebnisse liefern wissenschaftlich fundierte Informationen als Grundlage zur Bewertung und Einschätzung der Nutzung, der Leistungen und der Wirkungen der Jugendgerichtshilfe sowie allenfalls zu treffender Qualitätssicherungs- und Weiterentwicklungsmaßnahmen.

Projektleitung:
Universität Innsbruck

Projektpartner:
- Bundesministerium für Justiz

Kontakt:
Dr. Walter Hammerschick,
Mag.a Isabel Haider
Institut für angewandte Rechts- und Kriminalsoziologie,
Universität Innsbruck
Museumstraße 5/12
1070 Wien
Tel: +43 512 507 739 03
E-Mail: walter.hammerschick@uibk.ac.at
www.uibk.ac.at/irks/

KIIS

Künstliche Intelligenz im Strafvollzug

Das Projekt „Künstliche Intelligenz im Strafvollzug“ (KIIS) zielt darauf ab, ein intelligentes System zu entwickeln, das das Gefängnispersonal in seiner täglichen Arbeit unterstützt und den Schutz von Bediensteten und Inhaftierten vor physischer und psychischer Gewalt verbessert. Um dieses Ziel zu erreichen, nutzt das Projekt einen multimodalen Ansatz und greift auf fortschrittliche Technologien aus dem Bereich der künstlichen Intelligenz zurück.

Ein zentraler Fokus des Projekts liegt auf der Wahrung der Privatsphäre aller Beteiligten. Hierfür werden anonymisierende Sensortechnologien eingesetzt, wie beispielsweise Wearables oder 3D- und Thermalsensoren. Herkömmliche RGB-Kameras finden keine Verwendung. Durch die Integration verschiedener Datenquellen in ein konsistentes Fusionsmodell werden komplexe Verhaltensmuster erfasst. Das System erkennt nicht nur kritische Ereignisse, die sofortiges Eingreifen erfordern, sondern auch nonverbale Interaktionen und physische Kontakte.

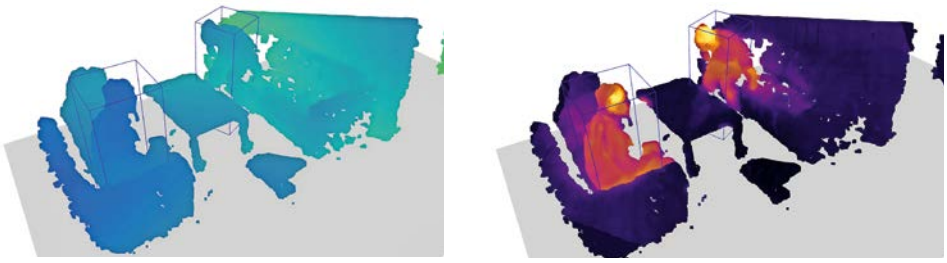


Abb.: 3D-Tiefendaten (links) und zugehörige Wärmebilddaten (rechts)

Im Rahmen des KIIS-Projekts wird eine umfassende Bewertung der Auswirkungen durchgeführt, einschließlich einer empirischen Bedarfs- und Risikoanalyse sowie einer juristischen Prüfung und ethischen Diskussion zur Zulässigkeit solcher Anwendungen. Diese Schritte gewährleisten, dass das KIIS-System den rechtlichen und ethischen Anforderungen entspricht und die Grund- und Menschenrechte respektiert. Um eine faire und transparente Verarbeitung sicherzustellen, werden die betroffenen Personen gemäß den ethischen Richtlinien und Bestimmungen der DSGVO umfassend über das Projekt informiert und über ihre Rechte informiert. Diese Informationen werden in klarer und einfacher Sprache schriftlich und mündlich kommuniziert.

Ein weiterer wichtiger Aspekt des KIIS-Projekts ist die Entwicklung eines „Explainable Artificial Intelligence (XAI)“-Systems. Das entwickelte System stellt dem Personal im Strafvollzug nicht nur nützliche Informationen zur Verfügung, sondern kann auch verständlich erklären, wie es zu bestimmten Schlussfolgerungen

oder Handlungsempfehlungen gekommen ist. Dadurch wird eine transparente und vertrauenswürdige Zusammenarbeit zwischen Mensch und Maschine ermöglicht.

Um die Verbreitung der erfassten Daten zu minimieren, wird im Rahmen des Projekts ein multimodaler Sensor entwickelt. Dieser Sensor vereint bildgebende Technologien wie Thermal- und Tiefenkomponenten in einem kompakten Formfaktor. Zudem verfügt das Modul über eine leistungsstarke Recheneinheit, die eine frühzeitige Datenfusion und lokale Ausführung von Deep-Learning-Modellen ermöglicht. Ein wesentlicher Vorteil dieses Ansatzes besteht darin, dass sensible Daten zu keinem Zeitpunkt das Gerät verlassen. Die Verwendung von anonymisierenden oder pseudonymisierenden Bildmodalitäten liefert einen zusätzlichen Schutz für die beteiligten Personen. Sowohl die Thermal- als auch die Tiefenmodalitäten ermöglichen keine Rückschlüsse auf die Identität der abgebildeten Personen.

Im Verlauf des Projekts wurden bedeutende Fortschritte erzielt. Die Entwicklung von spezialisierten Deep-Learning-Modellen, insbesondere ein Modell für simultane 3D-Erkennung und Tracking, geeignet für lokale sensornahe Ausführung, hat zu signifikanten Fortschritten geführt. Zudem wurde eine Kommunikationsschnittstelle zwischen cogvisAI Smartsensoren, der PKE AVASYS-Plattform und dem neu entwickelten Modell implementiert.

Ein weiterer bedeutender Aspekt des KIIS-Projekts liegt in der Entwicklung neuartiger Datensätze, die bisher in dieser Form nicht verfügbar waren. Diese Datensätze umfassen bimodale (Thermal- und Tiefenbilder) sowie trimodale (Thermal-, Tiefen- und RGB-Bilder) Aufnahmen. Zum einen wurden vor Ort in Justizanstalten Aufnahmen durchgeführt, um einen umfassenden Einblick in die zu erwartenden Interaktionen und Abläufe zu gewinnen. Neben diesen nicht öffentlichen Datensätzen wurden auch öffentlich zugängliche Datensätze außerhalb der Justizanstalten entwickelt, die sich auf komplexe und vielschichtige Interaktionen zwischen Personengruppen konzentrieren. Zusätzlich ergänzt werden diese Datenquellen durch synthetisch generierte Tiefen- und Thermobilder aus 3D-Modellen. Die Entwicklung eines diffusionsbasierten Rauschmodells ermöglicht es, realitätsnahe Bilder zu erzeugen.

Diese Datensätze bilden die Grundlage für die KI-Modelle, um Verhaltensmuster zu erkennen, kritische Ereignisse zu identifizieren und die Sicherheit in Justizanstalten zu verbessern. Die Entwicklung und Nutzung dieser Datensätze ermöglicht eine effektive Optimierung und Validierung der KI-Modelle, um eine zuverlässige Leistung zu gewährleisten.

Das KIIS-Projekt ist Teil einer umfassenden Initiative, Technologien zu erforschen, die zur Modernisierung des österreichischen Strafvollzugssystems beitragen können. Es strebt an, die hohen Standards des Strafvollzugs zu erfüllen und gleichzeitig die Privatsphäre, Rechtskonformität und ethischen Aspekte zu berücksichtigen.

Projektleitung:

Technische Universität Wien

Projektpartner:

- Bundesministerium für Justiz
- CogVis Software und Consulting GmbH
- PKE Holding AG
- Research Institute AG & Co KG

Kontakt:

PD. Dr. Martin Kampel
Computer Vision Lab,
Technische Universität Wien,
Institut 193/1
Favoritenstraße 9
1040 Wien

KI-SecAssist

KI basierte kooperative Luft- und Bodenrobotik zur Unterstützung von Einsatzkräften in Krisensituationen

Die steigende Anzahl von Krisen- und Katastrophensituationen sowie sich dynamisch ändernde Sicherheitslagen stellen immer größere Herausforderungen dar. Komplexe Einsatzstrategien, ein hoher Bedarf an Personalressourcen und deren Sicherheit erfordern eine orts- und zeitnahe sowie aufgabenoptimierte Assistenzleistung. Wesentliche Problemstellungen sind die echtzeitnahe Verfügbarkeit eines umfassenden Lagebildes, die aktuelle und detaillierte Information zu einzelnen Objekten (verletzte Person, Glutnestsituation, Temperatur-, Gaswerte etc.), um die zeitkritischen Entscheidungsprozesse für die notwendigen Maßnahmen unterstützen zu können, sowie ein Monitoring (Impact-Analyse) der gesetzten Maßnahmen, um gezielt weitere Unterstützungsmaßnahmen einleiten zu können. Kooperative Lösungsansätze mit mehreren unbemannten, (teil-)autonomen UAS- und UGV-Systemen bieten hier ein hohes Potenzial, wobei eine abgestimmte Funktionalität und Systemautonomie eine wesentliche Voraussetzung für eine optimierte Unterstützungsleistung darstellt.

Das Gesamtziel in KI-SecAssist ist ein modularer Proof-of-Concept-Funktionsdemonstrator, der die kooperative Nutzung verschiedenartiger UAVs und UGVs mit integrierter multisensoraler Payload unter Einsatz optimierter KI-basierter Datenprozessierungs- und Analysemethoden sowie intelligenten Koordinationsmodulen für eine direkte Unterstützung von Einsatzkräften nachweist.

Abb.: KI-basierte luft- und bodengestützte Assistenzsysteme für das Krisen- und Katastrophenmanagement

Die Anforderungen im Projekt fokussieren auf Waldbrandszenarien und den Schutz kritischer Infrastrukturen. Wesentliche Ziel und Entwicklungsschwerpunkte:

- UAVs- und UGVs-Koordination, Einsatzsteuerung und Management
  Einsatzorientierte Nutzung der Daten in einem dezentral verfügbaren Lagebild
- KI-basierte Datenprozessierung und Datenanalyse
  Innovative Analysemethoden zur Personendetektion und Glutnestkontrolle
- Multi-Sensordatenfusion, Situationsanalyse und dynamische Lagebildgenerierung
- Aufbau eines „Common World Models" als Grundlage für ein Aufgabenmanagement
- Dynamisches, kooperatives Aufgabenmanagement
  Automatisierte Verwaltung und Priorisierung von Aufgaben sowie Zuordnung an Robotersysteme
- Innovative, flexible Sensorplattformen für UAV- und UGV-Trägerplattformen
  Multi-Sensorlösungen und On-Board-Datenprozessierungshardware ermöglichen gezielte Datenanalysen und eine multimodale Taskautonomie
- KI-SecAssist-Testinfrastruktur für die notwendigen umfangreichen Tests mit UAVs und UGVs
- Sozialwissenschaftliche sowie rechtliche und ethische Aspekte
  Status-quo-Analyse inter-/nationaler Einsatzstrategien und technischer Anforderungen
- Internationaler Austausch im Rahmen eines „Exchange of Experts Workshop"

Systemkomponenten und Module

Leistungsfähige Module und Systemkomponenten ermöglichen kooperative multimodale Interaktionsstrategien zwischen mehreren UAVs, UGVs sowie den Einsatzteams und damit ein intelligentes Zusammenspiel der einzelnen System-Module zu einer optimierten Assistenzleistung für konkrete Aufgaben. Durch die klar definierten Einsatzstrategien ist ein „Human-in-the-loop"-Prozess ein integraler Bestandteil im kooperativen Aufgabenmanagement. Detaillierte Objektinformationen sowie die intelligente und rasche Erstellung eines großräumigen aktuellen Lagebildes auf Basis eines „Common World Models" bilden die Basis für die Unterstützung von Entscheidungsprozessen und der Einsatzführung und die zeit- und geoorientierte Grundlage für die Festlegung von Zielen und Aufgaben der involvierten (teil-) autonomen UAVs/UGVs.

Intelligente On-board-Lösungen, die Integration von auf die Aufgaben abgestimmter Sensorik (optische-, thermale- und Lidar-Sensoren), Kommunikationslösungen auf den UAVs und UGVs sowie KI-basierte Analyseansätze ermöglichen eine intelligente, szenarienorientierte Kooperation (Datenaufnahmen, Objektdetektion, Klassifikation etc.) zwischen den Agenten und einer echtzeitnahen Ableitung einsatzrelevanter Informationen für die Einsatzleitung bzw. Einsatzkräfte vor Ort. Der Einsatz eines leistungsfähigen UGV-Systems und eines UAVs mit Wasserstoffantrieb ermöglicht grundsätzlich einen mehrstündigen Einsatz. Ein nutzerfreundliches Aufgaben-, Steuer- und Datenmanagement ermöglicht eine effiziente Auftragsdefinition sowie die Überwachung und Interaktion mit den Agenten durch den verantwortlichen Operator („human-in-the-loop") unter Berücksichtigung erprobter Strategien und Managementabläufe. Nebenstehend abgebildete UAVs und UGVs werden im Rahmen von KI-SecAssist eingesetzt.

Projektleitung:

Joanneum Research

Projektpartner:

- AIT Austrian Institute of Technology GmbH
- Berufsfeuerwehr Graz
- Bundesministerium für Landesverteidigung
- Disaster Competence Network Austria – Kompetenznetzwerk für Katastrophenprävention
- Freiwillige Feuerwehr Gumpoldskirchen
- IFR – Ing. Richard Feischl
- HAWE Mattro GmbH
- Technische Universität Graz – Institut für Softwaretechnologie
- twins gmbh

Kontakt:

DI Alexander Almer
JOANNEUM RESEARCH –
Institut für Informations- und Kommunikationstechnologien
Steyrergasse 17
8010 Graz
Tel: +43 316 876 1738
E-Mail: alexander.almer@joanneum.at
www.joanneum.at/digital

KI-Secure

Künstliche Intelligenz für Multi-Sensorlösungen zur autonomen Sicherung Kritischer Infrastruktur

Der Schutz kritischer Infrastrukturen gewinnt vor dem Hintergrund zunehmender Bedrohungen durch Terroranschläge sowie wachsender Abhängigkeiten der Bevölkerung von funktionierenden Infrastrukturen international, aber auch in Österreich stark an Bedeutung. Innovative technische Assistenzsysteme sollen eine rasche, flexible Einsetzbarkeit und (teil-)autonome Unterstützung gewährleisten und es somit ermöglichen, große Bereiche mit geringem Personaleinsatz effektiv zu überwachen.

Abb.: Schematische Darstellung des multimodalen mobilen KI-Secure-Konzepts für echtzeitnahe Lagebildgenerierung auf Basis mobiler Multisensormasten und (teil-)autonomer UAVs

Zielsetzungen und Szenarien

Das Ziel in KI-Secure ist die (teil-)autonome 24/7-Unterstützung von Betreibern und Einsatzkräften beim „Schutz Kritischer Infrastrukturen". Verfolgt wurde die Entwicklung innovativer Lösungen für die (teil-)autonome, permanente Beobachtung und Analyse als sicherheitskritisch definierter räumlicher Bereiche auf Basis eines multimodalen und multisensoralen Systemansatzes ortsveränderbarer terrestrischer und (teil-)autonomer UAV-basierter Module. Szenarien- und nutzerorientierte Managementmodule ermöglichen dabei eine echtzeitnahe Erstellung eines Lagebildes für eine effiziente Unterstützung der Bodenteams. Die Ableitung relevanter Risikokategorien basierend auf Sicherheitsanalysen von Expertinnen und Experten sowie der Infrastrukturbetreiber war die Grundlage für die Definition der Szenarien sowie für die detaillierte Ableitung von Anforderungen an die Systemmodule. Hier wurden vor allem die Anforderungen der beiden Bedarfsträger MESSER AUSTRIA GmbH und VERBUND Hydro Power GmbH berücksichtigt und entsprechende Nutzerszenarien erarbeitet und analysiert sowie die für KI-Secure-relevanten und -realistischen Einsatzbereiche festgelegt. Für kleinräumige Industrieanlagen (wie z. B. MESSER Austria) wurden folgende Szenarien definiert:

- Überwachung kritischer Bereiche: parkende und fahrende Fahrzeuge (Lkw/Pkw).
- Überwachung von Abfüllstationen: sich nicht mehr bewegende Personen bzw. Personendetektion bei Austritt diverser Gase.
- Überwachung der Abfüllstationen bei unregelmäßigem Austritt von Gasen bzw. unkontrollierten Gaswolken.

Der Fokus bei großräumigen Infrastrukturen (z. B. Verbund-Stauseen) wurde auf folgende Szenarien gelegt:

- Monitoring von kritischen Zufahrtswegen/-straßen wegen Gefährdung durch Naturgefahren (Lawinen).
- Überwachung kritischer Zufahrtstraßen und Erkennen/Klassifizieren von Fahrzeugen (Pkw/Lkw).
- Perimeterüberwachung eines Infrastrukturobjekts mit dem Fokus auf Personen.
- Überwachung Grundablass Staumauer: Personenbewegung.

Systemkonzept und Module

Die Abbildung zeigt im Überblick das KI-Secure-Systemkonzept, welches auf Basis der definierten Anforderungen sowie festgelegten Szenarien erarbeitet wurde.

Folgende Module und Funktionalitäten wurden im Rahmen des Projektes realisiert:

- Statische Koordination, Pfadplanung und Aufgabenverteilung auf Basis vordefinierter Missionen und/oder von Analyseergebnissen.
- Autonome Navigation während des Start- und Landeprozederes durch Einbindung mehrerer Sensoren.
- Echtzeit-Kommunikation zwischen UAVs und Mastsystemen.
- Entwicklung und Integration multisensoraler Lösungen für ein UAV-System (optisch, thermal) und einer Mast-Lösung inklusive der Integration eines FMCW-Radarmoduls 24 GHz.
- Entwicklung einer performanten Datenprozessierung und innovativer Analysemethoden für optische und thermale Bilddaten als „On-board"- und „On-ground"-Lösung.
- Implementierung und Optimierung von Trackingalgorithmen für Radardaten.
- Multi-Sensordatenfusion und KI-basierte Situationsanalyse sowie Ableitung eines optimierten Thermalbildes für die visuelle Verifikation durch einen Operator.
- Entwicklung von Visualisierungs- und Interaktionskomponenten für die geo-orientierte Situationsdarstellung, die Einsatzsteuerung und Datenmanagement.

Umfangreiche Tests in freiem Gelände sowie der Flughalle der Universität Klagenfurt wurden durchgeführt.

Projektleitung:

JOANNEUM RESEARCH Forschungsges.mbH, DIGITAL

Projektpartner:

- Universität Klagenfurt, Institut für Intelligente Systemtechnologien
- Bundeskanzleramt der Republik Österreich
- Freiwillige Feuerwehr Gumpoldskirchen
- IFR – Ing. Richard Feischl
- INRAS/Joby Austria GmbH
- Lakeside Labs Gmbh
- Messer Austria GmbH
- twins GmbH
- Verbund Hydro Power GmbH
- Verein Gesellschaft für Europäische Politik

Kontakt:

DI Alexander Almer
JOANNEUM RESEARCH – DIGITAL – Institut für Digitale Technologien
Steyrergasse 17
8010 Graz
Tel: +43 316 876 1738
E-Mail: alexander.almer@joanneum.at
www.joanneum.at/digital

KITT

Künstliche Intelligenz zur Verbesserung der Sicherheit von Tunneln und Tunnelleitzentralen

Die fortschreitenden Entwicklungen im Bereich der Digitalisierung der Straße und ihrer Infrastruktur resultieren in einem immer stärker vernetzten und automatisierten Verkehr. Beteiligte Fahrzeuge dienen dabei zunehmend als wesentliche Informations- und Kommunikationsplattform. Das bringt große Potenziale mit sich, die Sicherheit und Verfügbarkeit der Straßeninfrastruktur im Allgemeinen bzw. von Tunneln im Speziellen deutlich zu erhöhen. Dies gelingt präventiv durch frühzeitige Erkennung von sich anbahnenden Ereignissen, noch bevor sie tatsächlich eintreten, sowie ausmaßmindernd durch rasches und zielgerichtetes Einleiten von Schutzmaßnahmen durch Tunnelleitzentralen. Insbesondere durch die Technologie der Cooperative Intelligent Transport Systems (C-ITS) stehen künftig zusätzliche Informationen zur Beurteilung der aktuellen Verkehrssituation und Sicherheitslage im Tunnel zur Verfügung. Diese ermöglicht den kontinuierlichen Austausch von Informationen zwischen Fahrzeugen und der Straßeninfrastruktur. Im Gegensatz zu sensorbasierten konventionellen Detektionssystemen, die nur auf die Auswirkungen von Ereignissen reagieren, ermöglicht die C-ITS-Technologie die direkte Erkennung der Ursachen. Den Potenzialen, die sich aus den zusätzlichen Informationen der Mobilitätsdaten ergeben, stehen große Herausforderungen gegenüber. Vor allem der Umgang mit den großen Datenmengen, wie die Überprüfung der Integrität sowie das systematische Selektieren, Zusammenführen, Analysieren und Auswerten, fordert den Einsatz automatisierter und effizienter Abläufe. An genau dieser Stelle kommt (schwache) künstliche Intelligenz (KI) zum Einsatz. Sie kann die Betreiber wesentlich dabei unterstützen, diese Datenflut effizient und zielgerichtet zu nutzen, um so beispielsweise Ereignisse vorab bzw. frühzeitig zu erkennen und spezifische Empfehlungen zu Sicherheitsmaßnahmen in Echtzeit bereitzustellen. In KITT werden die innovativen Werkzeuge C-ITS und KI zudem eingesetzt, um gängige Methoden der quantitativen Risikobewertung um wesentliche Aspekte zu erweitern. Derzeit basieren diese auf statischen Tunnelparametern (z. B. Tunnellänge, Querschnitt etc.) sowie auf Durchschnittswerten dynamischer Parameter (z. B. Verkehrsaufkommen, Lkw-Anteil, Fahrgeschwindigkeit etc.), die folglich zu jährlichen Durchschnittswerten für das Risiko führen. In einer Echtzeit-Risikoanalyse werden zusätzlich zu diesen standardmäßig verwendeten Werten auch dynamische Daten in Echtzeit herangezogen, die zu einem deutlich besseren Verständnis der aktuellen Situation im Tunnel führen. Diese Echtzeitdaten stammen sowohl aus den C-ITS-Daten als auch aus den bereits vorhandenen Tunnelsensorsystemen. Damit wird die Bewertung der Sicherheit in Straßentunneln in Echtzeit ermöglicht, und infolgedessen ein steuerndes Eingreifen, noch bevor das Ereignis tatsächlich eintritt. Somit können negative Auswirkungen abgemildert oder sogar zur Gänze vermieden werden.

Die Informationen zur aktuellen Sicherheitslage sowie die entsprechenden abgeleiteten Maßnahmenempfehlungen werden mittels eines eigens entwickelten Graphical User Interface (GUI) in übersichtlicher Form dem Tunneloperator in der Tunnelleitzentrale bereitgestellt, der in der Entscheidungsfindung in Stresssituationen damit deutlich unterstützt und entlastet wird. Die Weitergabe der Informationen an die Tunnelnutzer kann wiederum neben konventionellen Systemen der Tunnel- und Verkehrssteuerung (z. B. Wechselverkehrszeichen) auch über C-ITS erfolgen, welche einen bidirektionalen Datenaustausch sowohl im Normalbetrieb als auch im Ereignisfall ermöglicht. Im Vergleich zu herkömmlichen Systemen sind die Informationen nicht nur umfangreicher und spezifischer, sondern stehen auch unmittelbar und kontinuierlich über das gesamte Straßennetz zur Verfügung. Nicht zuletzt können auch die Einsatz- und Rettungsdienste, insbesondere die Feuerwehr, von den zusätzlichen und verbesserten Informationen profitieren, wie z. B. der exakten Lokalisierung von Ereignissen und der Angabe von beteiligten Fahrzeugtypen bei Unfällen im Tunnel. Ein wesentliches Ziel von KITT ist nicht zuletzt die frühzeitige Überprüfung relevanter rechtlicher und ethischer Aspekte, die sich aus den eingesetzten Technologien und neuen Entwicklungen im Projekt ergeben. Zwar ist die derzeitige Rechtslage zur Ausstattung und dem Betrieb von Straßentunneln bereits sehr umfangreich, aufgrund der rasanten technischen Entwicklungen, insbesondere im Bereich der Automatisierung und Vernetzung, ist jedoch eine Evaluierung und ggf. Anpassung bestehender Rechtsvorschriften erforderlich. Ziel ist, die rechtlichen Rahmenbedingungen zu definieren, um den wachsenden dynamischen Anforderungen gerecht zu werden. C-ITS bringt einen umfangreichen Datenaustausch zwischen den Fahrzeugen sowie zwischen Fahrzeugen und der Infrastruktur mit sich. Die Verarbeitung dieser großen Datenmengen, aber auch die neu eröffneten Kommunikationswege können zu Sicherheitslücken führen, die neben robusten technischen Lösungen auch entsprechende rechtliche und ethische Rahmenbedingungen erfordern.

Die Nutzung von C-ITS und die weitere KI-unterstützte Verarbeitung der zusätzlichen Informationen bringen erhebliche Potenziale zur Verbesserung der Tunnelsicherheit mit sich, sowohl hinsichtlich der Prävention von Unfällen als auch der verbesserten Reaktion im Ereignisfall durch optimiertes Notfallmanagement oder beschleunigte Selbst- und Fremdrettung.

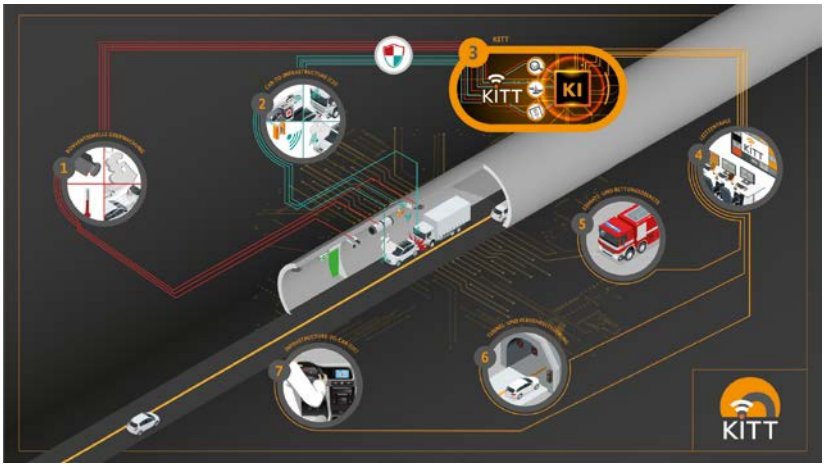


Abb.: KI hilft, die Sicherheit in Tunneln zu erhöhen

Projektleitung:

ILF Consulting Engineers Austria GmbH

Projektpartner:

- AIT Austrian Institute of Technology
- Universität Wien, Arbeitsgruppe Rechtsinformatik
- Österreichischer Bundesfeuerwehrverband
- Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft (ASFINAG)

Kontakt:

Dipl.-Ing. Bernhard Kohl
ILF Consulting Engineers Austria GmbH
Harrachstraße 26
4020 Linz
Tel: +43 512 2412 4213
E-Mail: info.linz@ilf.com
www.ilf.com

KRISAN

Entwicklung eines intelligenten automatisierten Notruf- und Abfragesystems für Krisensituationen

Bei der Bewältigung von Krisenfällen wie z. B. Pandemien werden Hotlines und Call-Center sowie die politische Führung und Behörden in organisatorischer, logistischer und emotionaler Sicht auf die Probe gestellt. Der Schutz der Bevölkerung hat dabei stets oberste Priorität. Im Krisenfall ist es derzeit jedoch für alle Beteiligten sehr schwierig, rasch einen Überblick über die Situation und ein gesichertes Lagebild zu erhalten.

Der Ausbruch der Covid-19-Pandemie hat eindrücklich verdeutlicht, dass eine rasche Datenaufnahme, die Erschließung zusätzlicher Informationsquellen und eine intelligente Zusammenführung zu einem echtzeitnahen Informationslagebild wesentlich sind, um kritischen Situationen rasch und effektiv zu begegnen bzw. verantwortungsvolle Entscheidungen treffen zu können.

Sprache ist die natürlichste und einfachste Kommunikationsform des Menschen. Mittels Sprachinformationen können rasch sehr komplexe Zusammenhänge beschrieben und daraus Schlüsse gezogen werden. Im Krisenfall treffen minütlich unzählige Telefonanrufe aus der Bevölkerung ein, die aufgrund fehlender Personalressourcen oft nicht verarbeitet werden können. In bestimmten Situationen sind die Leitungskapazitäten bzw. die Kapazitäten der verfügbaren Mitarbeiterinnen und Mitarbeiter in den Call-Centern erschöpft, wodurch mitunter hohe Wartezeiten für die Hilfeersuchenden entstehen.

Ziel des Projektvorschlags ist die Entwicklung eines Assistenzsystems zur automatisierten Anrufabfrage und echtzeitnahen Erstellung eines Informationslagebilds auf Basis von eingehenden Anrufen bei Leitstellen und Hotlines im Krisenfall. Durch eine automatisierte Auswertung der Anrufe können gleichzeitig Hunderte Anrufe von einem KI-basierten Sprachdialogsystem entgegengenommen werden. Durch eine automatisierte Anrufabfrage wird es möglich, die Informationen vieler Anrufe technisch elegant parallel zu analysieren. Dadurch wird vermieden, dass die Anruferin oder der Anrufer lange in der Warteschleife ausharren muss. Die Anruferin oder der Anrufer kann in natürlicher Umgangssprache die Informationen oder Fragen bekannt geben und das System extrahiert automatisch die nötigen Informationen. Das System generiert in Echtzeit je nach Gesprächsverlauf die passenden Fragen, um noch fehlende Informationen von der Anruferin oder dem Anrufer einzuholen. Im besten Fall erkennt die Anruferin oder der Anrufer im Gespräch nicht den Unterschied zwischen einer persönlichen Operatorin oder eines persönlichen Operators und dem Sprachdialogsystem. Die Thematik wird im Projekt in zwei unterschiedlichen Use-Cases untersucht. Einerseits soll ein bestehendes Notrufsystem, welches momentan über ein

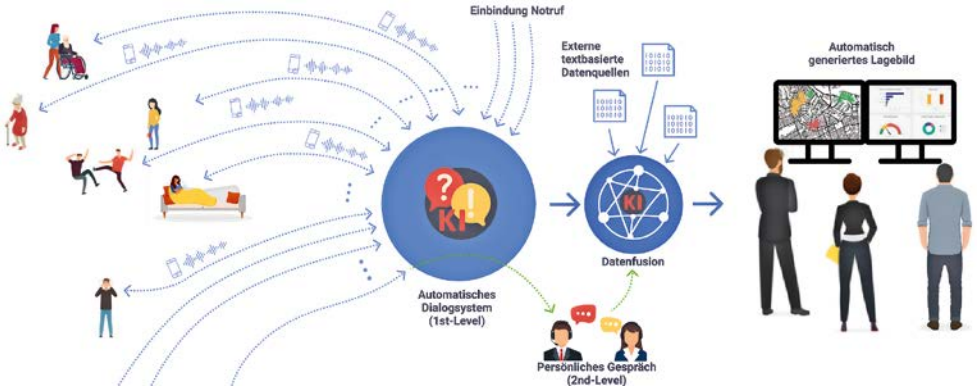


Abb.: Schematische Darstellung des geplanten Interaktionssystems

Call-Center abgewickelt wird, in einem vollautomatisierten Assistenzsystem mit KI-basiertem Sprachdialogsystem abgebildet werden. Dabei soll die Erfahrung von Expertinnen und Experten aus dem Call-Center verwendet werden, um das System bestmöglich für die Herausforderungen eines möglichen Echtzeitbetriebs zu entwickeln. Das Vorhandensein des realen Call-Center Notrufsystems ermöglicht es außerdem, das KI-basierte System mit realen Szenarien und Daten zu evaluieren und dadurch eine realistische Einschätzung seiner Einsatzmöglichkeiten zu erhalten.

Der zweite Use-Case behandelt eine fiktive Krisensituation in der Zukunft. Um die Bedarfsträger möglichst gut auf so eine Situation vorzubereiten, soll anhand von Beispielen aus der Vergangenheit (z.B. Covid-Pandemie) ein KI-Basissystem entwickelt werden, welches möglichst einfach an die jeweiligen Gegebenheiten angepasst werden kann. Da sich eine Krisensituation laufend verändert, muss ein solches System vom Bedarfsträger einfach angepasst und parametrisiert werden können. Dabei werden zu unterschiedlichen Zeitpunkten in der Krisensituation unterschiedliche Sachverhalte und Informationen für die potentiellen Anruferinnen und Anrufer relevant sein. Das im Projekt entwickelte KI-System soll daher, vom Bedarfsträger geführt, mit der fiktiven Krisensituation mitlernen und sich an die zum jeweiligen Zeitpunkt relevanten Informationen anpassen können.

Beide Use-Cases werden vom Projektteam gemeinsam mit Expertinnen und Experten aus dem jeweiligen Themengebiet entwickelt. Dabei ist es sehr wichtig, die relevanten Informationen vom User direkt in den Designprozess des technischen Systems einfließen zu lassen, sowie das Ergebnis in einer Feedbackschleife durch den User zu evaluieren. Durch dieses User-centered Design soll möglichst gut auf die Bedürfnisse der verschiedenen Usergruppen Rücksicht genommen werden können. Durch eine umfassende Akzeptanzanalyse wird weiters untersucht, inwiefern der Einsatz von KI bzw. eines Sprachdialogsystems von den Anruferinnen und Anrufern angenommen wird.
Schließlich werden die im Projekt behandelten Themen und Technologien hinsichtlich rechtlich-relevanter Aspekte bezüglich KI-Verordnungen und Datenschutz beleuchtet. So sollen die rechtlichen Richtlinien für einen Einsatz eines KI-basierten Sprachdialogsystem in Krisensituationen herausgearbeitet werden.

Projektleitung:

JOANNEUM RESEARCH Forschungsgesellschaft mbH

Projektpartner:

- Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
- DATAVIEW Handels- und Systemberatungs Ges.m.b.H.
- Österreichische Agentur für Gesundheit und Ernährungssicherheit GmbH
- Universität Wien Institut für Innovation und Digitalisierung im Recht
- Wiener Rotes Kreuz – Rettungs-, Krankentransport-, Pflege- und Betreuungsgesellschaft mbH
- youspi Consulting GmbH

Kontakt:

Dr. Ferdinand Fuhrmann
JOANNEUM RESEARCH – Institut für Informations- und Kommunikationstechnologie
Leonhardstraße 59
8010 Graz
Tel: +43 316 876 1309
E-Mail: ferdinand.fuhrmann@joanneum.at
www.joanneum.at

KRYPTOMONITOR

Verfahren zur forensischen Analyse von Smart Contracts und Off-Chain-Transaktionen

Das FFG-KIRAS-Projekt KRYPTOMONITOR, welches zwischen 2020–2022 erfolgreich abgeschlossen wurde, entwickelte Lösungen für die zunehmend als Tokens bzw. Smart Contracts umgesetzten virtuellen Vermögenswerte (Kryptoassets) sowie von Off-Chain-Zahlungskanälen. Das Ziel des KRYPTOMONITOR-Projekts lag in der Entwicklung generischer Kryptoasset-Analysemethoden, die neben nativen Kryptowährungs-Transaktionen auch die Analyse von Smart Contracts und Off-Chain-Transaktionen unterstützen. Die aus dem Projekt resultierenden Werkzeuge ermöglichen eine effektivere Strafverfolgung durch neue forensische Analyseverfahren und bieten eine faktenbasierte Entscheidungsgrundlage zur Bewertung möglicher Risiken und zur Durchsetzung regulatorischer Maßnahmen. Orthogonal dazu wurden im Projekt rechtliche und regulatorische Fragestellungen in Bezug auf Tokens beantwortet, Standards für einen effektiven Datenaustausch spezifiziert und Qualifizierungsstandards durch Schulungsmaßnahmen gesetzt. Im Folgenden werden spezifische Ziele und Projektergebnisse erläutert, die in KRYPTOMONITOR erreicht wurden.

Rechtliche Bewertung der entwickelten Methoden und Regulierungsempfehlungen hinsichtlich Tokens und Zahlungskanälen. Hier gilt es insbesondere Anwendungsbereiche sinnvoll abzustecken und die Datenflüsse so auszugestalten, dass Finanzbehörden möglichst hohen Nutzen im Steuerverfahren daraus ziehen können, dabei aber insbesondere die Grundsätze der Verhältnismäßigkeit und Datensparsamkeit gewahrt bleiben. Die Erkenntnisse dieser Arbeit umfassen eine Definition von Kryptoassets, eine Analyse zur steuerrechtlichen Behandlung von Mining-Pools, eine Abhandlung zu Meldepflichten bezüglich Wallet-IDs sowie einen Vorschlag zur Normierung von Datensicherungsmaßnahmen.

Neue forensische Methoden zur Analyse generischer Kryptoassets, die als Programmbibliotheken umgesetzt und in existierende Werkzeuge (GraphSense) integriert wurden. Im Rahmen des Projekts wurde ein neues Analyse-Werkzeug namens EtherSci entwickelt, das die Nachverfolgung von Werteflüssen auf Ethereum und bei ähnlichen Kryptowährungen ermöglicht, soweit dies möglich ist. Außerdem wurden aus Ethereum-Transaktionsdaten automatisiert Transaktions-Pfade und Muster extrahiert sowie die Häufigkeit der Nutzung von Services von kriminellen Akteuren quantifiziert. Des Weiteren wurde ein neues Analysewerkzeug entwickelt (Ethpector), das automatisiert relevante Informationen aus Smart-Contract-Programmen extrahiert und damit den Analyseprozess von bisher unbekannter Smart-Contract-Logik unterstützt

Systematische Analyse und Risikobewertung von Tokens. Ein besonderes Augenmerk lag dabei auf dem Risk-Report (RR)-Werkzeug von Ethpector, welches im Rahmen von KRYPTOMONITOR entwickelt wurde. Das Tool extrahiert automatisiert relevante Informationen aus Smart-Contract-Programmen und unterstützt damit den Analyseprozess von bisher unbekannter Smart-Contract-Logik. RR stellt eine einfache Oberfläche (UI und Report) zur Verfügung, um schnell einen Überblick über die Funktionalität eines Smart Contract zu erhalten. Zusätzlich werden risikobehaftete Eigenschaften, wie etwa Funktionen, welche virtuelle Währungseinheiten verwalten, als gesonderte Risikowarnungen ausgegeben. Mit RR wird die Risikobewertung von Smart Contracts vereinfacht und automatisierbar.

Formate für einen harmonisierten Datenaustausch zwischen involvierten Stakeholdern. Im zweiten Projektjahr wurde eine technische Spezifikation für standardisierte Datenaustauschformate zwischen Strafverfolgungs- und Regulierungsbehörden, Handelsplattformen und Kryptoforensikspezialisten bereitgestellt. Jegliche Form von Information (z. B. der Name einer Börse, eines Wallet-Anbieters usw.) zu einer Kryptowährungsadresse wird dabei in Form von sogenannten Tags gesammelt. Zusammengehörige Tags werden in TagPacks gesammelt: als TagPack definiert ist eine Struktur zum Sammeln und Koordinieren von Attributions-Tags mit Metadaten (z. B. zusätzliche Herkunftsinformationen, Zeitstempel, Vertrauensindex und Kategorisierung unter Verwendung der zuvor beschriebenen Taxonomien.

Ein abgestimmtes Curriculum als Qualifizierungsmaßnahme für Ermittler. Im September 2021 wurde ein erstes Training mit mehr als 50 Teilnehmerinnen und Teilnehmern aus allen österreichischen Bundesländern an der Universität Innsbruck durchgeführt. Ein zweites Training wurde im September 2021 am TechGate in Wien umgesetzt. Die erprobten Schulungsunterlagen wurden für einen Kryptoasset-Forensik-Lehrplan zur Verfügung gestellt und an der Bundesfinanzakademie für die bis Ende 2023 geplanten Kryptoasset-Forensik-Kurse ausgerollt.

Zu den Erfolgen des Projektes gehören die Gründung des Spin-offs Iknaio Cryptoasset Analytics GmbH (https://www.ikna.io/), welches den operativen Betrieb nach Projektende sicherstellt, sowie Medienberichte auf Servus TV („Fahndung Österreich“, Mai 2021) und in der Edition des österreichischen eco. nova-Magazins vom September 2021.

Projektleitung:

AIT Austrian Institute of Technology GmbH

Projektpartner:

- Universität Innsbruck – Security and Privacy Lab
- Research Institute GmbH
- T3K Forensics GmbH
- Bundesministerium für Inneres – Abt. II/BK/7 (Wirtschaftskriminalität)
- Bundesministerium für Finanzen – Abt. I/9 (Betrugsbekämpfung Steuer und Zoll)

Kontakt:

Dr. Bernhard Haslhofer
AIT Austrian Institute of Technology GmbH
Giefinggase 4
1210 Wien
Tel: +43 664 88390692
Email: bernhard.haslhofer@ait.ac.at
www.ait.ac.at/

LINK

Analyse und Nowcasting von Extremereignissen mithilfe von Richtfunkdaten

Infolge des Klimawandels nehmen extreme Wetterereignisse erheblich zu. Lokale und rechtzeitige genaue Kurzzeitvorhersagen – für maximal 12 Stunden – solcher Wetterereignisse bieten große Vorteile, denn sie ermöglichen die Durchführung geeigneter Gegenmaßnahmen zur Schadensminimierung sowie eine bessere Planung im Allgemeinen. Kurzfristige Vorhersagen erfordern ein dichtes Netz von Messungen, um aktuelle Wetterdaten zu erhalten. Solche Messungen können entweder von bodengebundenen Stationen oder von ferngesteuerten Systemen wie Wetterradar oder Satelliten stammen. In weiten Teilen Österreichs ist jedoch die Anzahl der Bodenstationen aufgrund des unwegsamen Geländes begrenzt, während Radardaten für bestimmte Regionen aus topografischen Gründen fehlen können. Im LINK-Projekt wurden physikalische Daten aus kommerziellen Richtfunknetzen (CML), wie sie in der Mobiltelefonie verwendet werden, genutzt, um genaue lokale Niederschlagsinformationen zu gewinnen. Dies liegt darin begründet, dass Niederschlagsdichte und Luftfeuchtigkeit mit der Abschwächung von CMLs korrelieren, wie bereits in vorangegangenen Forschungsarbeiten einiger Forschungsgruppen gezeigt werden konnte (siehe Abbildung). Allerdings waren 80-GHz-CMLs bis dato unbekanntes Terrain für die Abschätzung von Niederschlägen und Regenereignissen, außerdem waren die meisten bisherigen Ergebnisse auf Laborbedingungen beschränkt. Das 80-GHz-Frequenzband deckt dabei rund 75 % aller in Österreich aktiven Links ab, ist also für die Abdeckung ein wesentlicher Faktor. Der kontinuierliche Ausbau von CML-Netzen erzeugt große Mengen an Daten über die physikalischen Eigenschaften von Funkübertragungen über große Gebiete. Die Netzbetreiber messen diese Eigenschaften (z. B. den Verlust der Signalstärke bei der Übertragung zwischen den Antennen) routinemäßig, um die Netzqualität zu gewährleisten. Ziel des Projekts war es daher, die Verwendbarkeit von CML-Daten für die Vorhersage extremer Wetterereignisse zu bewerten.

Dazu war es notwendig, die CML-Rohdaten einer intensiven Analyse in Hinblick auf ihre Qualität und Fehlereigenschaften zu untersuchen. Wir entschieden uns dabei für einen Machine-Learning-basierten

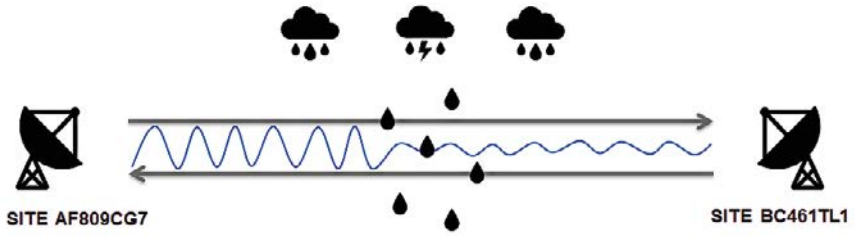


Abb.: Schematische Darstellung der Dämpfung

Ansatz. Die bereinigten Daten wurden im Anschluss zu 15-minütigen Zeitfenstern aggregiert und in numerische Wettervorhersagemodelle integriert, wobei einige Schritte in der Vorverarbeitung der Daten notwendig wurden. Die Basiswerte für Luftfeuchtigkeit und Niederschläge wurden während trockener Ereignisse gesammelt. Dazu wurden die INCA-Daten verwendet, die von der ZAMG bereitgestellt wurden. Diese Daten bestehen aus vielen Parametern für ein 701 x 501 km² großes Raster über Österreich und über die Landesgrenzen hinaus. Jeder Gitterpunkt dieser Daten enthält Niederschlag in mm, Temperatur, relative und spezifische Luftfeuchtigkeit sowohl für die untere Atmosphäre als auch 2 Meter über dem Boden, Windgeschwindigkeit und -richtung und vieles mehr. Zur Modellierung der topografischen Merkmale wurde ein Raster von 10 km² definiert. Um weitere Erkenntnisse über die zu bestimmten Zeiten beobachteten Signale zu gewinnen, berechneten wir den Extinktionskoeffizienten anhand des Beer-Lambertschen Gesetzes. Damit erhielten wir einen Koeffizienten, der die Auslöschung des Signals beschreibt, die durch die Länge der Verbindung und die Substanz, die das Signal durchquert, verursacht wird, in unserem Fall die Luft in einer bestimmten Höhe, in der das CML positioniert ist. Auf diese Weise ist es möglich, drei der wichtigsten Merkmale, nämlich die Sendeleistung, die Empfangsleistung und die Distanz zwischen den Links, in einer einzigen Variablen zu kombinieren.

Auf Basis dieser neuen, CML-integrierten Modelle wurden Vorhersagen getroffen bzw. auch sog. Now-Casting, die Errechnung von aktuellen Niederschlagsereignissen, betrieben. In der Evaluierung war dieses Modell in der Lage, Regenereignisse mit einer Genauigkeit von über 97 % vorherzusagen, wobei sich weniger als 1 % der 120.000 Testbeobachtungen als false positives und weniger als 5 % als false negatives erwiesen, was angesichts des rechentechnisch performanten Modells ein gutes Ergebnis ist. Gleichzeitig war es dadurch umgekehrt auch möglich, Störungen und Leistungsabfälle im Netz auf lokale Wetterphänomene zurückführen zu können.

Im Projekt konnte gezeigt werden, dass die erforschten Ergebnisse zur Nutzbarkeit von Mikrowellendaten und deren Verwendung in einem Vorhersagemodell von hohem Interesse für den numerischen Wetterschutz sind. Weiters konnte gezeigt werden, dass die Nutzung von Sekundäreffekten in CML auch in realen Umgebungen mit derzeit vorhandener und standardmäßig eingesetzten Technologien Ergebnisse sinnvoller Genauigkeit liefert. Speziell in der Landwirtschaft konnten so Anwendungsfelder identifiziert werden, die von unseren neuen Methoden profitieren könnten. Die Mobilfunkanbieter wiederum profitieren von den neu entwickelten Methoden und Erkenntnissen, wie die KI-basierte Kombination von Wetter- und Mikrowellendaten genutzt werden kann, um Ausfälle und Störungen eindeutig Wetterphänomenen zuzuordnen und entsprechende technische Maßnahmen abzuleiten.

Projektleitung:

Fachhochschule St. Pölten ForschungsGmbH

Projektpartner:

- Zentralanstalt für Meteorologie und Geodynamik
- Hutchison Drei Austria GmbH
- FH St. Pölten GmbH, Institut für Medienwirtschaft (GSK-Partner)
- Amt der Steiermärkischen Landesregierung, Abteilung 14 – Wasserwirtschaft, Ressourcen und Nachhaltigkeit, Referat Hydrographie (Bedarfsträger)

Kontakt:

Oliver Eigner
Institut für IT Sicherheitsforschung, FH St. Pölten
Matthias-Corvinus-Straße 15
3100 St. Pölten
Tel: +43 2742 313 228 691
E-Mail: oliver.eigner@fhstp.ac.at
www.isf.fhstp.ac.at/

MEASURE

Monitoring Exercises using AI-Support for Reliable Evaluation

Notfälle und Katastrophen gut bewältigen zu können bedeutet für Einsatzorganisationen, regelmäßig für den Ernstfall zu trainieren. Dies geschieht unter möglichst realistischen Bedingungen, um Einsatzkräften ein effektives Lernerlebnis zu bieten und praxisnahe Erkenntnisse generieren zu können, die bei echten Notsituationen von entscheidender Bedeutung sind. Sie fließen in die Gestaltung neuer Taktiken und Ausrüstungsgegenstände ein und werden benötigt, um Ausbildungsinhalte anzupassen. Um zu aussagekräftigen Ergebnissen zu gelangen, ist allerdings eine engmaschige Beobachtung und eine valide, objektive Interpretation der Übungsgeschehnisse erforderlich. Dies erfordert derzeit hohen Zeit- und Ressourcenaufwand. Zusätzlich sind die Ergebnisse durch die subjektive Wahrnehmung der Evaluatorinnen und Evaluatoren geprägt. MEASURE untersucht die Anwendbarkeit diverser sensorbasierter Technologien sowie den Einsatz künstlicher Intelligenz (Sprachanalyse) sowie von mehrdimensionalen Analysen von Sensorsignalen, um eine aussagekräftigere und schneller verfügbare Evaluierung von Einsatzübungen zu ermöglichen. Dabei liegt, neben der technischen Anwendbarkeit, der Fokus auf der Anwendertauglichkeit für Evaluatorinnen und Evaluatoren von Einsatzorganisationen und auf den rechtlich/ethischen Rahmenbedingungen, die bei der Nutzung neuer Technologien in diesem Kontext noch wenig erforscht wurden.
Das Projekt ist wie folgt aufgebaut: Arbeitspaket 1 umfasst alle übergeordneten Koordinations-, Kommunikations- und Qualitätsmanagementaufgaben innerhalb des Projektes sowie die Koordination und Durchführung der wissenschaftlichen Dissemination und wirtschaftlichen Verwertung der Ergebnisse.
Arbeitspaket 2 befasst sich mit Anforderungsanalyse und Systemarchitektur. Im Rahmen dieses Arbeitspakets wird die Basis für die Entwicklung der Evaluierungsmethoden und -werkzeuge erarbeitet. Im Mittelpunkt steht die Identifizierung zentraler Erfolgskriterien (sog. „Key Performance Indicators“) und Leistungskennzahlen. Zusätzlich werden zu deckende Bedürfnisse der Anwenderinnen und Anwender sowie geeignete Settings für die automatisierte Evaluierungsunterstützung bestimmt. Auf Basis dieser Erkenntnisse wird die Gestaltung der Systemarchitektur vorbereitet.
Die Erkenntnisse aus diesem Arbeitspaket werden in Arbeitspaket 3 – Planung und Beurteilung – genutzt, um eine modellbasierte Methode zur Übungsevaluierung zu entwickeln. Diese Methode soll unter anderem folgende Hauptaspekte unterstützen:

- Erstellung eines Übungsüberblickes in Bezug auf Ablauf, Schwerpunkte, erwartete Ergebnisse und Evaluierung;
- Darstellung von Szenen und zusammenhängenden Szenarien;
- Modellierung der Übungsziele, der messbaren Kennzahlen sowie der notwendigen Datenanbindung; und
- Spezifikation der Datenanbindung mittels On-site-Sensoren.

Darüber hinaus soll ein praktikabler, digitaler und modellbasierter Proof-of-Concept zur Übungsevaluation geschaffen werden. Parallel zu Arbeitspaket 3 laufen die Aktivitäten im Arbeitspaket 4 – Sensorik und Analytik. Einzelne Tätigkeiten und Ereignisse, die in Einsatzübungen vorgesehen sind, werden in diesem Arbeitspaket untersucht und relevante Größen gemessen. Dafür wird ein Portfolio unterschiedlicher Sensortechnologien verwendet, um Datensätze messtechnisch zu erfassen und zu übertragen. Weiters sollen damit auch Erkenntnisse über die Tauglichkeit getesteter Sensortechnologien durch die Erhebung und Auswertung von Messdaten während Einsatzübungen gewonnen werden.

Arbeitspaket 5 dient der Evaluierung der in den vorherigen Arbeitspaketen erarbeiteten Werkzeuge. Diese werden in iterativen Feldtests, sogenannten Testbeds, anhand definierter KPI (re-)evaluiert und begleitend zu den Labortests weiterentwickelt. Zudem erfolgt ein finaler Test im Rahmen einer Einsatzübung kurz vor Projektende, vor allem hinsichtlich ihrer Tauglichkeit und Leistungsfähigkeit, gegenüber den bereits definierten Anforderungen. Die gewonnenen Erkenntnisse werden gesammelt, dokumentiert und zusammengefasst und in einem abschließenden Evaluierungsbericht aufbereitet.

Aufgrund der geringen bzw. aktuell unüblichen Nutzung der im Projekt untersuchten Technologien im Kontext der Leistungsüberprüfung von Einsatzkräften ergeben sich Fragestellungen in Bezug auf die zu berücksichtigenden rechtlichen und ethischen Rahmenbedingungen in Arbeitspaket 6. Dabei werden in diesem Arbeitspaket insbesondere Aspekte im Bereich des Datenschutzrechts und des Einsatzes von künstlicher Intelligenz dargestellt. Zusätzlich werden Besonderheiten des gegebenen Übungskontexts, wie etwa der Verpflichtung zur Fortbildung nach dem Sanitätergesetz (SanG) und Aspekte des Katastrophenschutzrechts, besonders herausgearbeitet. Auf dieser Basis wird der aktuelle Rechtsrahmen evaluiert und werden allfällige Empfehlungen zur Anpassung und Erweiterung ausgesprochen.

m Sicherheitsforschungs-Förderprogramm KIRAS des Bundesministeriums für Finanzen, startete am 1.11.2022 und läuft bis 31.10.2024.

Abb.: Foto von einem Lego Serious Play © Workshops im Arbeitspaket 2 – Anforderungsanalyse und Systemarchitektur – mit Anwenderinnen und Anwendern

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- BOC Products & Services AG
- Disaster Competence Network Austria
- Fachhochschule Technikum Wien
- Stadtfeuerwehr Pinkafeld
- Landesfeuerwehrverband Steiermark
- Österreichisches Rotes Kreuz
- Universität Wien, Institut für Europarecht, Internationales Recht und Rechtsvergleichung

Kontakt:

Bernhard Bürger, MSc
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 664 8839 0704
E-Mail: bernhard.buerger@ait.ac.at
www.ait.ac.at/

MEDIAS

Mediation als Instrument der Streitbeilegung und Konfliktlösung: Anwendungspraxis und Effekte

1. Thematischer Rahmen

Die Gewährleistung von Rechtssicherheit und Rechtsfrieden als öffentlichem Gut stellen zentrale Ziele der Zivilgerichtsbarkeit dar. Prozessrecht und Gerichtsbarkeit dienen zugleich dem Schutz der gesamten Rechtsordnung und sind Fundamente der öffentlichen Sicherheit, der Zivilgerichtsbarkeit kommt bei dieser (rechts-)staatlichen Aufgabe enorme Bedeutung zu. Vor Gericht zu gehen ist allerdings in der Regel das letzte Mittel (ultima ratio). Vielen Konflikten liegen Probleme auf der Kommunikations- und Beziehungsebene zugrunde, die in formalen Gerichtsverfahren meist nur ungenügend berücksichtigt werden können. Diese können vielmehr tendenziell eskalationsfördernde Interaktionen verstärken. Die teils hohen psychischen und sozialen Folgekosten gerichtlicher Streitbeilegung können durch hohe materielle Kosten und zeitlich langwierige Verfahren negativ verstärkt werden.

Die Grenzen und Risiken gerichtlicher Streitentscheidung beförderte die (Weiter-)Entwicklung von alternativen Konfliktlösungsverfahren (Alternative Dispute Resolution – ADR). Die Mediation als international anerkanntes Verfahren der konsensorientierten Konfliktlösung (Win-win-Lösungen) ist hier ein besonders wichtiger Ansatz. In bestimmten Konfliktfeldern und -konstellationen können solche Verfahren nachhaltigere und dem Rechtsfrieden förderlichere Konfliktlösungen bieten und in der Folge zur Konfliktprävention beitragen.

In Österreich wurde 2004 mit dem Zivilrechts-Mediations-Gesetz (ZivMediatG) vergleichsweise früh ein rechtlicher Rahmen für Mediation in Zivilrechtssachen geschaffen. Das Gesetz legt u. a. Standards für die Aus- und Weiterbildung von Mediatorinnen und Mediatoren fest, die in Verbindung mit der vom Justizministerium geführten Liste eingetragener Mediatorinnen und Mediatoren zur Qualitätssicherung der Mediation beitragen sollen. Das ZivMediatG ist auf außergerichtliche Kontexte beschränkt, während in Deutschland auch die Möglichkeit gerichtsinterner Mediation in der Zivilprozessordnung rechtlich verankert ist. Doch auch in Österreich erproben einzelne Richterinnen und Richter den Einsatz von Mediation oder mediationsähnlicher Instrumente alternativer Streitbeilegung bei gerichtsanhängigen Verfahren.

2. Erkenntnisinteresse und Zielsetzungen

Bis dato fehlt systematisches Wissen über die Nachfrage und Akzeptanz von Mediation in Österreich sowie über Verfahrens- und Ergebnisqualität als auch Effekte der durchgeführten Mediationen. Die im März 2023 gestartete KIRAS-Studie MEDIAS erhebt erstmals für Österreich umfassende und aus-

sagekräftige empirische Daten zur Anwendungspraxis, Qualität und Wirksamkeit außergerichtlicher Mediation gemäß ZivMediatG. Die Studienergebnisse werden 2025 vorliegen und bieten die Basis für eine evidenzbasierte Weiterentwicklung mediativer Verfahren der Konfliktvermittlung und der rechtlichen Rahmenbedingungen. Wichtig ist dabei auch, das Wechselverhältnis zwischen Mediation und Zivilgerichtsbarkeit zu analysieren. Die Studie untersucht deshalb ergänzend auch Erfahrungen mit Mediation bei gerichtsanhängigen Verfahren in Österreich. Die empirischen Ergebnisse sollen zu einem förderlichen Ergänzungsverhältnis zwischen mediativen Verfahren der Streitbeilegung und der Rechtskontrolle durch staatliche Zivilgerichte beitragen.

3. Methodik

Die Forschungsziele werden durch einen komplexen Forschungszugang (Between-Method-Triangulation) erreicht, bei dem unterschiedliche quantitative und qualitative Methoden im Sinne einer wechselseitigen Ergänzung mehrfach miteinander verschränkt sind (Mixed Methods). In einer abschließenden Projektphase werden die gewonnenen Ergebnisse systematisch und praxiswirksam zentralen Stakeholdern vermittelt. Das Forschungsdesign und die darin integrierten methodischen Zugangsweisen sind in nachfolgender Grafik visualisiert.

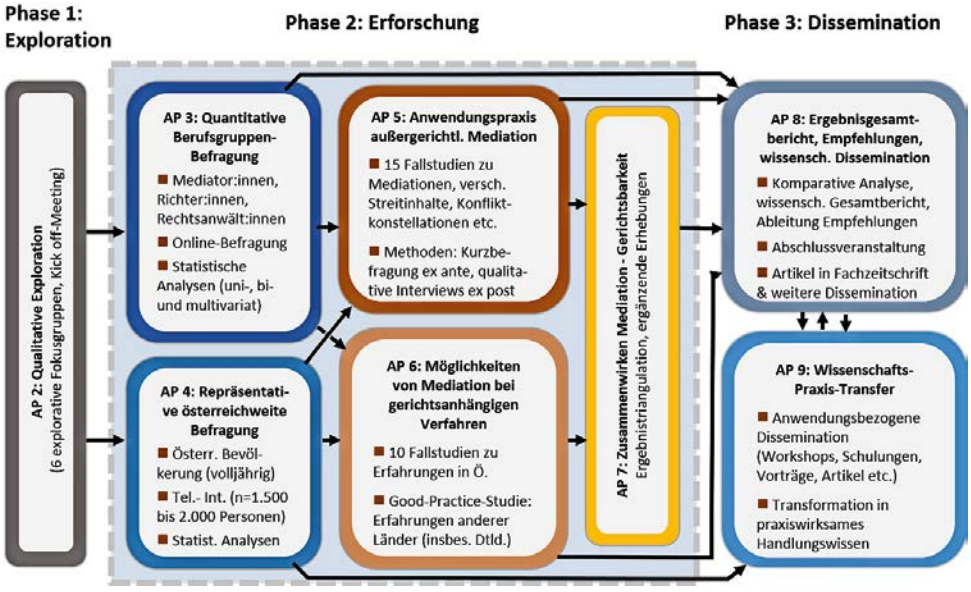


Abb.: Projektaufbau und Forschungsdesign MEDIAS

Projektleitung:

Institut für angewandte Rechts- und Kriminalsoziologie, Universität Innsbruck

Projektpartner:

- Bundesministerium für Justiz

Kontakt:

Ass.-Prof. Dr. Hemma Mayrhofer
IRKS – Institut für angewandte Rechts- und Kriminalsoziologie
Universität Innsbruck
Museumstraße 5/12
1070 Wien
Tel: +43 512 507 73902
E-Mail: hemma.mayrhofer@uibk.ac.at
www.uibk.ac.at/irks/

MRespond

Multi-User Mixed Reality System für flexibles Training von Einsatzkräften

Mixed Reality Trainingssystems zur Erweiterung der Trainingsmöglichkeiten für Einsatzorganisationen, um eine bessere Vorbereitung auf den Ernstfall für Führungskräfte und operative Einheiten zu schaffen.

Für Ersthelfer von Feuerwehr, Rettung und Bundesheer ist effektives Handeln und das richtige Einschätzen von Gefahrensituationen – besonders in Großschadenseinsätzen – essenziell. Zur Erlangung dieser Fähigkeiten sind großflächige Trainings mit unterschiedlichen Ersthelfern in möglichst realistischer Umgebung nötig. Häufig sind solche Szenarien jedoch zu gefährlich, teuer oder aufwendig, um sie realistisch genug nachzustellen – was den Trainingsnutzen schmälert. Mixed-Reality (MR)-Technologien können virtuelle Gefahren innerhalb einer physischen Trainingsumgebung realistisch darstellen. Zurzeit existieren vereinzelt Lösungen mit MR-Konzepten, diese bieten jedoch unzureichend Bewegungsfreiheit. Die Interaktion zwischen Ersthelfern bzw. realen/virtuellen Objekten kommt zu kurz.

Anpassungsmöglichkeiten für die Übungsleitung – um verschiedene Varianten eines Szenarios zu üben – sind begrenzt. Ziel von MRespond ist es, Technologien zu erforschen, welche eine wesentliche Verbesserung für MR-Trainings im Bereich Bewegungsfreiheit, Interaktion und dynamischer Anpassbarkeit herbeiführen. Deren Einsatztauglichkeit wird mit Unterstützung der Bedarfsträger geprüft. Dazu werden zwei großflächige Einsatzszenarien – ein Gebäudebrand sowie ein Szenario mit chemischen Gefahren – erarbeitet und umgesetzt. Führungs- und operative Einsatzkräfte müssen interdisziplinär Gefahrensituationen bewältigen. Hauptaugenmerk liegt hier auf der freien Beweglichkeit aller Trainierenden in Außen- und mehrstöckigen Innenbereichen, der Interaktion zwischen realen und virtuellen Gegenständen (z. B. für die Nutzung gewohnter Ausrüstung) sowie der Adaptierbarkeit der Szenarien. Dafür bedarf es der Konzeption einer robusten Lokalisierung und Verfolgung der Trainierenden in Außen- und Innenbereich sowie geeigneter Objekterkennungsalgorithmen. Sowohl sichtbare (Feuer, Rauch, …) als auch unsichtbare Gefahren (z.B. chemische Stoffe, erkennbar mit Messgeräten) können virtuell im Gelände platziert werden. Notfallpuppen stellen Verletzte dar und werden zur Darstellung realistischer Verletzungsmuster mit virtuellen Verletzungen überblendet.

Handlungen der Trainierenden haben Einfluss auf virtuelle Elemente (z. B. Rauchabzug bei Fensteröffnung, Triage-Entscheidungen). Ein Übungsleiterinterface ermöglicht es, den Trainingsablauf zu adaptieren, Gefahren zu platzieren und Handlungen zu bewerten. Die Akzeptanz von Trainings mit virtuellen Elementen, Trainingswirksamkeit sowie rechtliche Aspekte zu Übungsnormen untersucht.

Das MRespond Trainingssystem ermöglicht es 8 Personen gleichzeitig am Training teilzunehmen – je ein Einsatzleiter der Feuerwehr und einer Rettungsorganisation, 2 operative Einsatzkräfte je Organisation sowie einem Trainer je Organisation. Das System besteht aus mehreren Komponenten:

MR-Trainingsapplikation: Die Trainierenden sind mit einer Magic Leap One MR Brille ausgestattet. Die Trainierenden sehen virtuelle Gefahren (Feuer, Rauch, chemische Flüssigkeit) an der richtigen Position und können zusammenarbeiten, um die Gefahr zu beseitigen. Reale Rettungspuppen werden erkannt und mit virtuellen Verletzungen überblendet. Diese müssen aus dem Gebäude gerettet werden. Rettungskräfte müssen Triage-Entscheidungen treffen und die Patienten und Patientinnen versorgen. Aktionen der Trainierenden (z.B. Öffnen eines Fensters, richtige Versorgung) haben einen Einfluss auf das Brandverhalten sowie den Vitalzustand der Patienten und Patientinnen. Reale Objekte (Strahlrohr, Türen, Fenster, Rettungspuppen) werden erkannt und in das Training eingebunden.

Übungsleiterinterface: Trainer und Trainerinnen sind mit einem Tablet ausgestattet. Sie können über das entwickelte Übungsleiterinterface die Position der Trainierenden verfolgen, Gefahren platzieren sowie Verletzungsmuster und die Vitalparameter der simulierten Patienten- und Patientinnen adaptieren. Diese können mit den Trainierenden sprechen.

Serverapplikation: Eine Serverapplikation sammelt die Daten aller Sensoren (Strahlrohr, Fenster, Türen, Rettungspuppen), aus der Trainingsapplikation sowie den Inputs des Übungsleiterinterfaces und leitet die relevanten Informationen an die MR-Trainingsapplikationen und Übungsleiterinterfaces weiter.

Das System wurde im Zuge des Projektes von End-Usern des Roten Kreuzes, der Berufsfeuerwehr Linz sowie des BMLV in 2 Zwischenevaluierungsworkshops und einem Endevaluierungsworkshop auf dem Trainingsgelände der BF Linz demonstriert und evaluiert.

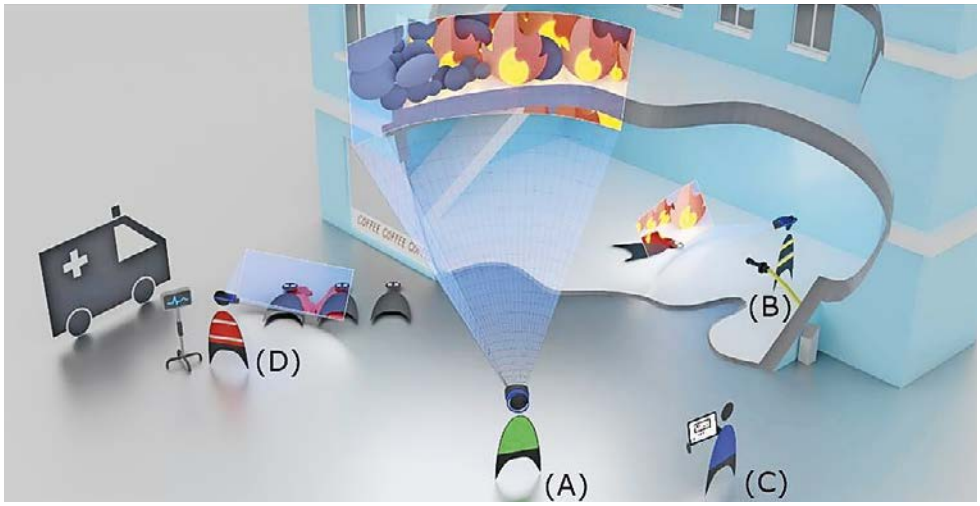


Abb.: Trainierende können sich frei in einem mehrstöckigen Gebäude sowie dem umliegenden Außenbereich bewegen. Führungskräfte der Feuerwehr können die Lage von außen beurteilen (A) und die Einsatzkräfte in das Gebäude schicken. Die Einsatzkräfte der Feuerwehr können gefährliche Situationen mit ihrer gewohnten Ausrüstung bekämpfen (z. B. Löschen eines virtuellen Feuers mittels realen Feuerwehrschlauchs) (B). Übungsleiterinnen und Übungsleiter können die Position von allen Trainierenden in einem Übungsleiterinterface sehen, virtuelle Gefahren platzieren sowie Gesundheitsparameter und virtuelle Verletzungen während des Trainings verändern (C). Für das Üben von Triage-Szenarien werden virtuelle Gefahren auf Notfallpuppen projiziert. Sanitäterinnen und Sanitäter können wie gewohnt Wunden versorgen (D). Das Trainingsszenario passt sich weiters den Handlungen der Trainierenden an (z. B. das Öffnen eines realen Fensters verändert das virtuelle Brandverhalten).

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Technische Universität Wien
- Berufsfeuerwehr Linz
- Österreichisches Rotes Kreuz
- Bundesministerium für Landesverteidigung
- Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH
- MINDCONSOLE GmbH

Kontakt:

Elisabeth Broneder
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 664 825 1374

MUSIG

Multisensor-basierte Informationsgenerierung zur Unterstützung von Krisenmanagement und Präventionsstrategien

Das MUSIG-Projekt fokussiert auf die automatisierte, KI-basierte Ableitung und Fusion von Bewegungsinformationen aus geosozialen Medien, Mobilfunkdaten und In-situ-Kamerabildern. Diese fusionierte Bewegungsinformation wird anschließend mit Kontextinformation (semantischen Themen und Stimmungen aus geosozialen Medien, Bewegungsgeschwindigkeiten und Personendichten aus In-situ-Bilddaten) angereichert und in Echtszenarien auf ihren Mehrwert im Krisenmanagement und deren Prävention getestet.

Projekthintergrund und Ziele

Kollektive Massenbewegungen von Menschen und Aktivitäten im öffentlichen Raum stellen Behörden und Einsatzkräfte zunehmend vor große Herausforderungen in Bezug auf Lageerfassung, Krisenmanagement und -prävention. Ereignisse in der jüngeren Vergangenheit wie der Sturm auf das US-Kapitol, Menschenversammlungen trotz nicht genehmigter Demonstrationen, nicht eingehaltene Ausgangsbeschränkungen während Pandemien etc. zeigen die Relevanz und Dringlichkeit dieser Thematik.

Deshalb fokussiert das MUSIG-Projekt auf automatisierte Extraktion kollektiver Bewegungsinformation aus geosozialen Medien, Mobilfunkdaten und In-situ-Bilddaten mit KI-Methoden und der szenarienorientierten Fusion der Bewegungsinformation in einem neuartigen Mixed-methods-Ansatz sowie deren Bereitstellung für Krisenmanagement und -prävention in naher Echtzeit inkl. Nowcasting-Information.

Durch die Fusionierung von Bewegungsinformation aus heterogenen Quellen entsteht so eine hochqualitative und verlässliche Informationsbasis, die belastbar in Krisenmanagement und -prävention einsetzbar ist. Über die reine Bewegungsanalyse (Ermittlung von Personenanzahl, -dichte und Bewegungsgeschwindigkeit) hinaus extrahiert das MUSIG-Projekt semantische Information (worüber sprechen Menschen in einer Gruppe?) und Stimmungsinformation (Sentiment-Analyse – wie entspannt, angespannt, eskalierend etc. ist die Stimmung in einer Gruppe?) in folgenden methodischen Ansätzen:

- Erforschung von robusten und transparenten KI-Algorithmen für multisensorale Analyse von Bewegungsinformation (Personenanzahl, -verteilung, -dichte und Verhalten) aus geosozialen Medien, Mobilfunkdaten und In-situ-Bilddaten.
- Erforschung eines Mixed-methods-Ansatzes zur Zusammenführung von Bewegungsinformationen: Fusion von heterogenen Informationsebenen – aus Mobilfunk- und Bilddaten gewonnene Personendichten und Bewegungsgeschwindigkeiten, aus geosozialen Medien extrahierte geogra-

fisch und zeitlich lokalisierte Emotionen (Stimmungen – Sentiment Analysis) und sich dynamisch verändernde Gesprächsthemen (Nowcasting).

- Rechtliche, soziologische und ethische Fragestellungen sind zentraler Teil des MUSIG-Projektes (Ethical Board) und werden in den techn. Entwicklungen reflektiert.
- Bedarfe von Endanwendern werden strukturiert wissenschaftlich erhoben und praxisnah erprobt (2 „Cold Cases", 1 „Warm Case") in einer TRL-4-Testumgebung, und Interoperabilität mit bestehenden Systemen wird gewährleistet.
- Erarbeitung einer umfassenden Verwertungsstrategie mit klarem Commitment zur Entwicklung einer gemeinsamen Dienstleistung über das Projektende hinaus.

Fusion von Bewegungsdaten und Contextual Enrichment

Die Forschungsergebnisse des MUSIG-Projektes umfassen neue Methoden und Algorithmen für die Extraktion von Bewegungsinformation aus geosozialen Medien, Mobilfunkdaten und Bilddaten. Die Abbildung zeigt Hotspots von aus Mobilfunkdaten extrahierten Personendichten (oben), den Zeitverlauf der Anzahl von Personen in zwei geografischen Gebieten (Mitte) und aus Bilddaten abgeleitete Personendichten (unten). Darüber hinaus werden Methoden für die Generierung von semantischer und Sentiment-Information erforscht, mit deren Hilfe die Bewegungsinformationen kontextualisiert werden.

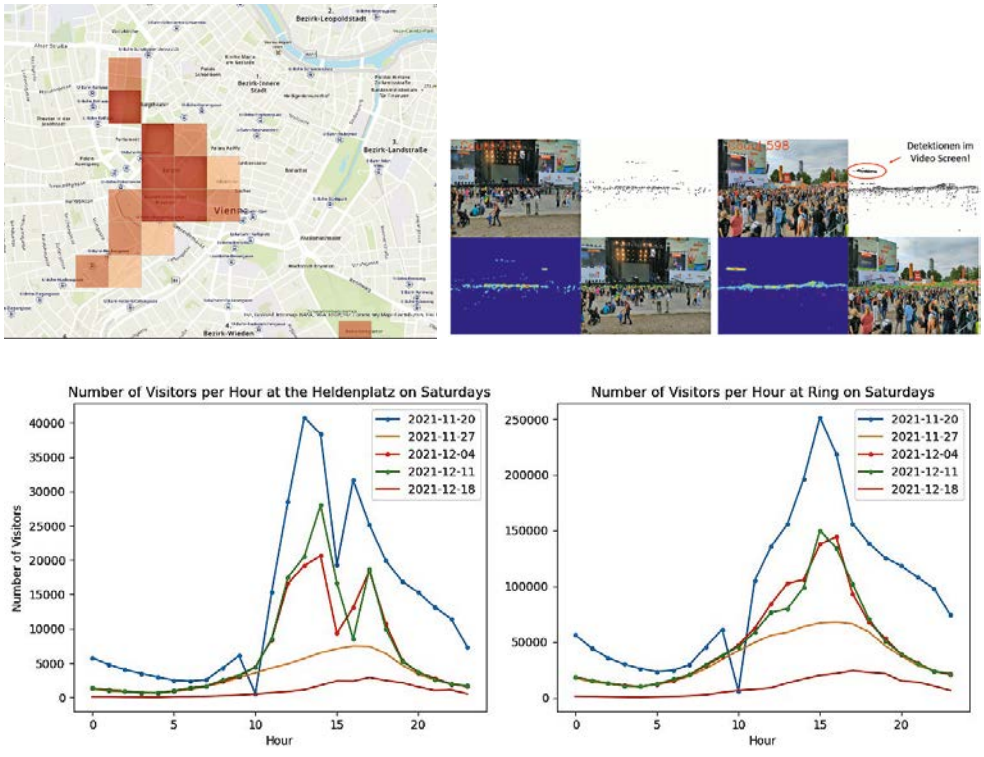


Abb.: Informationsextraktion aus geosozialen Medien, Mobilfunkdaten und Bilddaten

Projektleitung:

Paris-Lodron-Universität Salzburg

Projektpartner:

- Universität Salzburg, Fachbereich Geoinformatik – Z_GIS
- Österreichisches Rotes Kreuz
- Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH
- Spatial Services GmbH
- JOANNEUM RESEARCH
- eurofunk KAPPACHER GmbH
- Bundesministerium für Inneres
- Hutchison Drei Austria GmbH
- Disaster Competence Network Austria

Kontakt:

Assoz.-Prof. Dr. Bernd Resch
Universität Salzburg, Fachbereich Geoinformatik – Z_GIS
Schillerstraße 30
5020 Salzburg
Tel: +43 662 8044 7551
E-Mail: bernd.resch@plus.ac.at
www.zgis.at

NIKE MED

Nachhaltige Interdisziplinarität bei Komplexen Einsätzen MEDizinische Versorgung

Das Projekt NIKE MED verfolgt das Ziel, im Falle eines Untertage-Katastropheneinsatzes die notfallmedizinische Versorgung sowie die Erstellung von Kapazitätenkarten unter Einbeziehung der psychosozialen Komponenten zu optimieren. Ein Massenanfall unter Tage stellt dabei eine große Herausforderung. Zu den besonderen Herausforderungen zählen die rasche Erstversorgung, das Triagieren, die Zuweisung zur richtigen Versorgungskette und die möglichst rasche Verbringung zur fachärztlichen Definitivversorgung in spezialisierten medizinischen Einrichtungen unter Ausnützung der verfügbaren nationalen und internationalen Kapazitäten.

Dazu wurde eine Applikation für alle involvierten Einsatzkräfte entwickelt, um die Zielorte der Patientinnen und Patienten sowie die Disposition der bestgeeigneten Transportmittel durchführen zu können. Ziel ist die Unterstützung einer möglichst raschen Definitivversorgung. NIKE MED leistet damit einen essenziellen Beitrag zum Erreichen der vollen Einsatzbereitschaft einer spezialisierten Einsatzgruppe mit der Befähigung zum Einsatz unter Tage und damit einen essenziellen Mehrwert für das Staatliche Krisen- und Katastrophenmanagement. Dazu arbeiten im Projekt der Lehrstuhl für Subsurface Engineering der Montanuniversität Leoben, das Bundesministerium für Landesverteidigung, das Disaster Competence Network Austria – Kompetenznetzwerk und Katastrophenprävention, die IL Ingenieurbüro Laabmayr & Partner ZT GmbH, die Mindconsole GmbH, das Institut für Psychologie der Universität Innsbruck und das Clinical Skills Center der Medizinischen Universität Graz zusammen.

Zur Erreichung dieses Ziels wurden alle User-Requirements der verschiedenen Akteure, vom Einsatzleiter bis hin zur Sanitäterin, erfasst und davon abgeleitet wurde eine Applikation erstellt, welche Daten von Einsätzen erfassen kann, eine Kommunikation zwischen Einsatzeinheiten und Einsatzleitern ermöglicht, Lageänderungen live unter den Einheiten teilt, Versorgungspfade von Patientinnen und Patienten erfassen kann, gesetzte Maßnahmen einzelner Einheiten basierend auf vorhandenen Systemen erfassen kann, das Arbeiten in Großschadenslagen vereinfacht und die Kommunikation zwischen Einheiten fördert und damit die Patientenversorgung bei Großschadenslagen unter Tage vereinfacht.

Die Erfassung und Analyse von Konzepten für die psychosoziale Unterstützung von Einsatzkräften wurde mittels Literaturanalyse abgearbeitet. Dabei wurden von 437 Publikationen 39 für die nähere Analyse als geeignet empfunden. Fazit ist, dass es zur Unterstützung von Einsatzkräften nach belastenden Einsätzen zwar viele Konzepte gibt, aber die Datenlage für Untertage-Einsätze nicht gut ist. Aus diesem Grund wurden Experten-Interviews und Fokusgruppendiskussionen durchgeführt. Aus den daraus gesammelten Erkenntnissen konnten Empfehlungen für Einsatzkräfte in den uns interessierenden Lagen und für Notfälle unter Tage gewonnen werden. Zudem wurden anhand des EU-Projektes OPSIC auf Basis der von

über 300 psychosozialen Richtlinien erstellten Comprehensive Guideline die allgemeinen Richtlinien zur Einsatzkräfte- und Betroffenenbetreuung zusammengefasst dargestellt.

Die Funktionen und die Menüführung der Einsatzleiter-Applikation, die von Mindconsole programmiert wurde, wurde von Übungsteilnehmern inkl. Polizei und Feuerwehr auf Tablets im Hörsaal getestet. Im Vordergrund stand dabei die Erstellung eines Designprototypen, der einen digitalen Zwilling hinsichtlich der Abläufe, Kriterien und Parameter eines durchgängigen notfallmedizinischen Versorgungsprozesses von der Auffindung des Patienten bzw. der Patientin an der Schadstelle über die Triage und den Transport bis zur erfolgreichen Übergabe des Patienten in der richtigen Schwerpunkteinrichtung darstellt.

Im Rahmen einer 1:1-Übung im Straßentunnelsystem am ZaB – Zentrum am Berg, die am 16.9.2023 stattfand, wurde die Einsatzleiter-App in einem Unfallszenario im Realmaßstab getestet und deren Verwendbarkeit für Notfallorganisationen im Einsatzfall auf einer Tablet-Hardware geprüft. Dabei stand die Personenregistrierung durch die verschiedenen Einsatzorganisationen mit unterschiedlichen Zeitstempeln im Fokus. Durch das Testen der App im Rahmen der 1:1-Untertage-Übung wird gewährleistet, dass die zentrale Grundfunktion der Applikation auf einer ersten prototypischen Ebene überprüft wird und ob und wie ein digitales Vernetzungssystem mit einem bestehenden analogen System funktionieren kann.

Das Zentrum am Berg (ZaB) ist ein Forschungs-, Entwicklungs- und Seminarzentrum der Montanuniversität Leoben für den Bau und Betrieb unterirdischer Anlagen. Darüber hinaus ist es als Trainings- und Ausbildungszentrum für Rettungsorganisationen und für Personal konzipiert, das in Betrieb, Wartung und Instandhaltung der Verkehrsinfrastruktur beschäftigt ist.

Auf Basis der Arbeiten im Rahmen des NIKE-MED-Projektes lassen sich noch weitere Empfehlungen ableiten:

- Sämtliche Informationen müssen rasch, klar und kohärent sein,
- das Personal muss gut trainiert sein,
- zwischen den Einsatzorganisationen muss es klare Rollenaufteilungen geben,
- technische und bauliche Details spielen bei der Panikverhütung eine große Rolle,
- die Betroffenen unter Tage müssen befähigt werden, die Kommunikation nach außen aufrechtzuerhalten.

Abschließend kann festgehalten werden, dass alle Stakeholder einen großen Vorteil in der Umsetzung einer organisations- und professionsübergreifenden Applikation sehen.

Abb.: Einsatzübung im Straßentunnelsystem am ZaB – Zentrum am Berg der Montanuniversität Leoben

Projektleitung:

Montanuniversität Leoben

Projektpartner:

- Bundesministerium für Landesverteidigung
- DCNA – Disaster Competence Network Austria
- IL – Ingenieurbüro Laabmayr & Partner ZT GmbH
- Mindconsole GmbH
- Clinical Skills Center der Medizinischen Universität Graz
- Universität Innsbruck – Institut für Psychologie

Kontakt:

Univ.-Prof. Robert Galler
Montanuniversität Leoben
Erzherzog Johann Straße 3
8700 Leoben
Tel: +43 3842 402 3401
E-Mail: Robert.galler@unileoben.ac.at
www.zab.at

NIKE – SubMoveCon

Nachhaltige Interdisziplinarität bei Komplexen Einsätzen unter Tage – Subsurface Movement Control

Motivation und Problemstellung

Der Schutz kritischer Transportinfrastrukturen gewinnt zunehmend an Bedeutung. Bedrohungsanalysen dokumentieren, dass aufgrund der geschlossenen Situation in U-Bahn-Stationen erhebliche Hindernisse für die sichere und effiziente Evakuierung von Personen nach einem Anschlag zu berücksichtigen sind.
Ziel von NIKE-SubMoveCon ist es, auf Basis eines multidisziplinären Ansatzes im Bereich der Sensorik, automatisationsgestützter Analysen multisensoraler Daten, technischer Assistenzsysteme und Managementlösungen sowie sozialwissenschaftlichen Aspekten wesentliche Forschungs- und Entwicklungsergebnisse zu erarbeiten und damit die Sicherheit in Untertage-Terrorsituationen zu erhöhen.
Die Entwicklungen ermöglichen den Einsatz von intelligenten, mobilen und tragbaren Multisensor-Lösungen (optische-, thermale-, akustische Sensorik, Gas-Sensoren etc.) unmittelbar vor Ort und am Menschen (Human Sensor) sowie die echtzeitnahe Generierung eines 3-D-Gesamtlagebildes. Auf Basis eines echtzeitnahen Lagebildes sowie technischer Assistenzsysteme wird eine optimierte Einsatzführung ermöglicht und somit die Sicherheit der involvierten zivilen Personen als auch der Einsatzkräfte wesentlich erhöht (siehe Abb. 1).

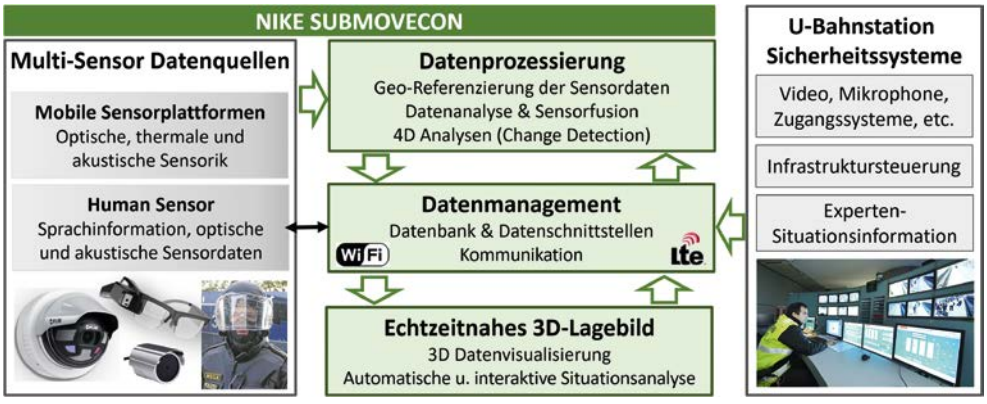


Abb. 1: Modulübersicht NIKE-SubMoveCon.

Forschungsschwerpunkte und Ergebnisse

Aufgrund der Unübersichtlichkeit in unterirdischen Strukturen war es das Ziel, ein geoorientiertes Einsatzleitsystem zu implementieren, das Informationen und Analyseergebnisse in Form eines 3-D-Lagebildsystems verständlich zur Verfügung stellt. Die Ergebnisse der multisensoralen Datenanalyse aus Akustik und bildgebender Sensorik sowie der mobilen Human-Sensor-Applikation wurden echtzeitnah

räumlich in einem 3-D-Modell des Einsatzraumes dargestellt. Der Einsatz einer Virtual-Reality-Ansicht ermöglichte darüber hinaus eine Erkundung des Einsatzgebietes, was wesentlich zum Verständnis der unterirdischen Strukturen beiträgt.

Augenmerk wurde auf die Objektdetektion aus optischen und thermalen Videokameras gelegt, wobei in NIKE-SubMoveCon Personen und Fahrzeuge besonders wichtig sind. Im Projekt wurden Algorithmen entwickelt, die mithilfe von künstlicher Intelligenz diese Objekte robust in Echtzeit detektieren und auch über die Zeit verfolgen können. Im Falle von Personen wurde zusätzlich die Pose berechnet, um potenziell verletzte liegende Personen erkennen zu können. Die räumliche Lage der Personen wurde dann direkt an das 3-D-Lagebild inkl. einer Klassifikation in stehend, gehend, laufend bzw. liegend übergeben.

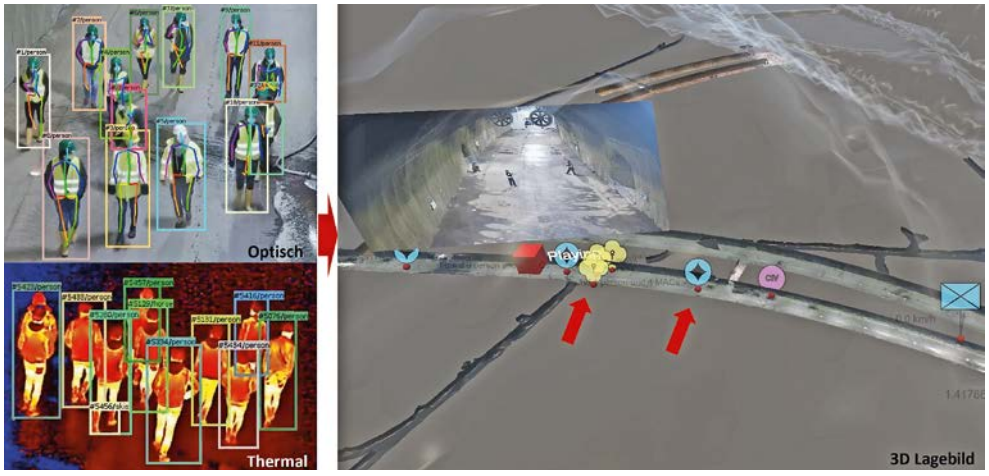


Abb. 2: Detektion, Verfolgung und Klassifikation von Personen und Fahrzeugen aus optischen und thermalen Videodaten (l.) sowie Visualisierung der Detektionen im 3-D-Lagebild (r.)

Ziel der akustischen Datenauswertung war es, Schreie und Gespräche sowie Schüsse zu erkennen und zu lokalisieren. Die entwickelte Detektion funktioniert über eine Auswahl von Audio-Merkmalen und einer folgenden Event-Detektion. Die räumliche Lokalisierung wurde mit einer direkten Zuordnung zum nächstgelegenen Mikrofon als auch über eine Triangulierung umgesetzt, sodass die Audio-Events direkt im 3-D-Lagebild visualisiert werden konnten.

Um Lageinformationen direkt am Ort des Geschehens zu erhalten, wurde eine Human-Sensor-Applikation realisiert, die aus einer mobilen, personengetragenen Multisensorlösung und einer multimodalen Verarbeitungs- und Übertragungskomponente besteht. Dieses mobile Informationssystem kombiniert eine am Helm getragene Kamera, ein Audio-Streaming-Set sowie textilintegrierte Biosensorik, die in der Lage ist, Vitaldaten sowie die Position des Trägers zu erfassen und zu verarbeiten. Die verarbeiteten Audioereignisse (Schreie, Schusserkennung etc.), der Videostream der Helmkamera sowie die Vitaldaten (Herzfrequenz, Atemfrequenz, Temperatur und Belastungsindex) werden in Echtzeit an das 3-D-Lagebildsystem übertragen und ermöglichen die Verfolgung der Position und des Belastungszustandes der Einsatzkräfte.

Projektleitung:

JOANNEUM RESEARCH Forschungsges.mbH, DIGITAL

Projektpartner:

- Bundesministerium für Landesverteidigung
- Montanuniversität Leoben
- IFR – Ing. Feischl Richard
- IL-Ingenieurbüro Laabmayr & Partner ZT GesmbH.
- ERC Experience Research & Consulting e.U.
- Verein des Grünen Kreuzes Krankentransport- und Unfalldienst Steiermark

Kontakt:

DI Alexander Almer
JOANNEUM RESEARCH – DIGITAL – Institut für Informations- und Kommunikationstechnologien
Steyrergasse 17
8010 Graz
Tel: +43 316 876 1738
E-Mail: alexander.almer@joanneum.at
www.joanneum.at/digital

NoiseSens

Entwicklung und Evaluierung eines multimodalen Messsystems zur Identifizierung von Lärmsündern im Straßenverkehr.

Die Anzahl der Motor- und Tuningbegeisterten ist in den letzten Jahren stark angestiegen. So finden in den größeren Städten regelmäßig illegale Straßenrennen statt, die einerseits überaus gefährlich für andere Straßenteilnehmer und andererseits durch die Lärmentwicklung sehr störend sind. Durch diverse Veränderungen am Motor und der Auspuffanlage werden extrem laute Knalle produziert, die weithin hörbar und für die Anrainer eine enorme Belastung darstellen. Am stärksten ist das Bundesland Kärnten betroffen, wo jedes Jahr Tausende Motor- und Tuningbegeisterte das Bundesland bevölkern. Für die Polizei wird es immer schwieriger, während dieser Zeit die öffentliche Sicherheit und Ordnung aufrechtzuerhalten und die Bevölkerung zu schützen. Einerseits betrifft dieser Schutz die Abwehr von Vandalismusakten sowie die Verhinderung gefährlicher Situationen im Straßenverkehr. Ein anderer Fokus liegt aber natürlich auf der Erhaltung von „Ruhe und Ordnung".
Für Ruhe kann die Exekutive allerdings immer weniger sorgen, da ihnen derzeit die technischen Möglichkeiten fehlen, mittels geeigneter Messgeräte die Vergehen der Tunerinnen und Tuner auch zu ahnden, indem die Straftat auch der entsprechenden Fahrerin, dem entsprechenden Fahrer bzw. dem Fahrzeug zugeordnet werden kann. Durch die große Anzahl an Fahrzeugen und dem unübersichtlichen Geschehen ist eine eindeutige, gerichtsfeste Zuordnung meist nicht möglich. Derzeit existiert kein Messgerät, das die Anforderungen der Polizei erfüllt und gerichtsfeste Beweise für die Verstöße von Tunerinnen und Tunern während Auto-Events liefert.

Ziel des vorliegenden Projektvorschlags ist es daher, ein multisensorales Messgerät zu entwickeln und zu testen, das es künftig der Polizei erlaubt, gerichtsfeste Beweise im Zuge von Tuning-Events zu sichern. Dieses mobile Messgerät soll aus einer Kombination von akustischer Sensorik, visueller und Thermalsensorik und einem Abstandssensor bestehen. Die akustische Sensorik besteht aus einem kommerziell erhältlichen geeichten Schallpegelmesser und einem Mikrofonarray. Die örtliche Zuordnung der Lärmemission zu einem Fahrzeug soll mit einem Mikrofonarray, einer visuellen Kamera und einer Thermal-Kamera erfolgen. Der Abstand zwischen dem Messgerät und der betreffenden Schallquelle soll mittels einer herkömmlichen Laserpistole gemessen werden. Die Kenntnis des Abstands ist für die Schallausbreitungsrechnung nötig, da der tatsächliche Schalldruckpegel am Fahrzeug immer nur auf einen bestimmten Abstand zum Sensor und dessen gemessenen Pegel bezogen werden kann.

Im Zuge des Projekts sollen die einzelnen Sensoren in ein Gesamtsystem integriert werden, sodass Tests und Demonstrationen in Echtzeit möglich sind. Das konzipierte Gesamtsystem soll mobil einsetzbar sein,

sodass die Sensoren vor Ort von Polizistinnen und Polizisten einfach und rasch installiert und bedient werden können. Die erhaltenen Messergebnisse werden einem in Fahrtrichtung postierten Anhaltetrupp der Polizei in Echtzeit auf ein Tablet/Mobiltelefon übermittelt, sodass diese die betreffenden Kfz-Lenkerinnen und -lenker mit den objektiven Messergebnissen bzw. Beweisen konfrontieren und die weiteren Maßnahmen (z. B. Abnahme der Kennzeichen) einleiten können.

Die relevanten Ereignisse im akustischen und visuellen Bereich (Knalle, Stichflammen, etc.) sollen dabei von der Sensorik automatisch erkannt und dem Verursacherfahrzeug zugewiesen werden. Dazu sollen entsprechende Modelle des maschinellen Lernens entwickelt werden, welche anhand von vorgegebenen Beispielen angelernt werden. Um relevante akustische und visuelle Daten zu sammeln werden im Projekt bei einschlägigen Veranstaltungen der Tuning- und Bikerszene Messungen durchgeführt. Die dabei erhobenen Daten werden anschließend gesichtet und die relevanten Ereignisse extrahiert. Mit diesen aufgearbeiteten Daten werden die statistischen Modelle des maschinellen Lernens trainiert, welche die relevanten Ereignisse während des Echtzeitbetriebs des zu entwickelnden Messgerätes erkennen können. Im Projekt werden auch die sozio-demographischen Bereiche der Thematik beleuchtete. So werden Befragungen der involvierten Nutzergruppen (Anrainer, Verursacher und Exekutive) durchgeführt, um die jeweiligen Bedürfnisse zu erheben. Auf dieser Basis sollen weitere Erkenntnisse gewonnen werden, welche in die Entwicklung von zukünftigen Richtlinien in der Verkehrsordnung in Bezug auf Lärmemissionen einfließen sollen.

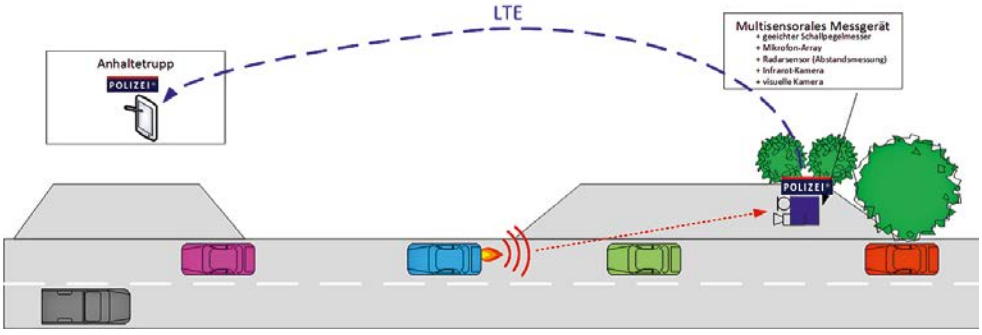


Abb.: Einsatz des geplanten Messgeräts mit Anhaltetrupp der Polizei

Projektleitung:

JOANNEUM RESEARCH Forschungsgesellschaft mbH

Projektpartner:

- AMT DER KÄRNTNER LANDESREGIERUNG, Abteilung 7 – Wirtschaft, Tourismus und Mobilität, A07 Verkehrsrecht und Verkehrsunternehmen
- Lakeside Labs GmbH
- Hottinger Brüel & Kjaer Austria GmbH
- Schuster + Schuster Traffic Infrastructure Consulting GmbH
- Bundesministerium für Inneres

Kontakt:

Dr. Ferdinand Fuhrmann
JOANNEUM RESEARCH
Leonhardstraße 59
8010 Graz
Tel: +43 316 876 1309
E-Mail: ferdinand.fuhrmann@joanneum.at
www.joanneum.at

PCS

Plattform Compliance Studie

Die weitreichende Anwendung von künstlicher Intelligenz und Algorithmen durch Plattformen und Online-Dienste verändert die digitale Erfahrungswelt von Konsumentinnen und Konsumenten grundlegend. Über die ermöglichten komplexen Datenanalysen können automatisiert die Reihung von Produkten, die Anzeige von Empfehlungen, Werbung, Preise oder auch das User-Experience-Design (UX) von Websites selbst angepasst werden. Diese wird als teilweise notwendig erachtet, um zum Beispiel in der schieren Menge an Information den passenden Überblick zu schaffen. Gleichzeitig bringt Personalisierung auch Risiken mit sich – z. B. Diskriminierung und Intransparenz –, und diese Nachteile betreffen nicht alle Konsumentinnen und Konsumenten gleichermaßen.

Vor allem vulnerable Konsumentinnen und Konsumenten sind betroffen: Vulnerabilität wird dabei von der Europäischen Kommission situativ definiert. Zwar sind statistisch gesehen manche Gruppen der Bevölkerung öfters davon betroffen, z. B. Kinder und Frauen. Doch Vulnerabilität hängt nicht nur von soziodemografischen Kriterien ab, sondern auch mit dem persönlichen Verhalten (z. B. Hang zu Impulsivität), der persönlichen Situation sowie dem Marktkontext zusammen. Die Sicherheitsrisiken für vor allem Konsumentinnen und Konsumenten in ihrer Vulnerabilität umfassen die unrechtmäßige Verwendung und Verknüpfung von Daten, um Prozesse irreführend, manipulativ bzw. täuschend zu gestalten und um verhaltensbasierte Inhalte zu platzieren. Da diese Prozesse oft im Hintergrund passieren, ohne das bewusste Verständnis oder aktive Eingreifen der Userinnen und User, besteht der Bedarf, diese Praktiken aufzudecken.

Im Konsumentenschutz auf EU-Ebene werden diese datengesteuerten algorithmischen Vorgänge rund um Entscheidungsfindung, Ranking und Prozessgestaltung derzeit verstärkt mit dem Fokus auf Dark Patterns und verhaltensbasierter Werbung problematisiert. Es besteht ein wachsender Bedarf an Methoden und Tools, die im Bereich der Rechtsdurchsetzung zur Detektion und Dokumentation von Verstößen in diesem Sinne eingesetzt werden können.
Vor diesem Hintergrund wurde die vorliegende Studie konzipiert, als eine umfassende Analyse von unlauteren Geschäftspraktiken auf für Konsumentinnen und Konsumenten in Österreich relevanten Websites. PCS legt den Fokus auf eine Analyse von unlauteren Geschäftspraktiken im Sinne von Dark Patterns und verhaltensbasierter Werbung mit einem Konsortium von Expertinnen und Experten des Konsumentenschutzes, KI-Forscherinnen und -Forschern sowie dem BMSGPK.

Das Projektteam des ÖIAT (Österreichisches Institut für Angewandte Telekommunikation) untersucht mit dem AIT (Austrian Institute for Technology) und dem Bedarfsträger BMSGPK (Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz) die Phänomene Dark Patterns und verhaltensbasierte Werbung im Rahmen des KIRAS-Projekts „PCS – Plattform Compliance Studie“. Das Ziel ist, über Recherche, Tool-Entwicklung und eine Erhebung zu evaluieren, mit welchen Methoden und Tools eine Detektion und Dokumentation von Verstößen im Sinne von Verbraucherbehörden gelingen kann. Das Projekt wird zwischen Jänner 2023 und Juni 2024 (Laufzeit 18 Monate) durchgeführt.

In einem ersten Schritt erfolgt eine Erhebung und Messung von Verstößen im Sinne unlauterer Geschäftspraktiken mit Fokus auf Dark Patterns und verhaltensbasierter Werbung auf für österreichische Konsumentinnen und Konsumenten relevanten Plattformen und Online-Diensten. Darauf folgt eine Evaluation von vorhandenen Tools und Methoden für die Dokumentation und Beweissicherung durch Verbraucherbehörden und -organisationen. Aufbauend darauf wird eine Machbarkeitsstudie eines Tools für die Detektion und die Dokumentation von Dark Patterns und verhaltensbasierter Werbung durchgeführt, die Ergebnisse werden kumuliert in einem Studienbericht veröffentlicht. Das Ziel ist, damit einen Beitrag zu leisten, mit dem Konsumentenschutz im digitalen Zeitalter effektiver gegen Verstöße vorgehen kann.

Abb.: Schutz vor Dark Patterns für Konsumentinnen und Konsumenten

Projektleitung:

Österr. Institut für angewandte Telekommunikation

Projektpartner:

- AIT DSS Centre
- Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (Bedarfsträger)

Kontakt:

Louise Beltzung
Österreichisches Institut für angewandte Telekommunikation ÖIAT
Ungargasse 64–66/3/404
1030 Wien
Tel: +43 1 595 2112
E-Mail: beltzung@oiat.at
www.oiat.at

PINPOINT

Nationales Risikomanagement für GSVP Missionen unter Verwendung von OSINT und PNT Monitoring

Die Europäische Union (EU) führt derzeit 18 umfassende militärische und zivile Missionen und Operationen durch, die strategisch darauf ausgerichtet sind, kritische Probleme in verschiedenen Regionen zu lösen, die mit grenzbezogenen Herausforderungen oder Konflikten konfrontiert sind. Österreich hat sich im Rahmen dieser Missionen proaktiv an insgesamt acht Operationen im europäischen Kontext beteiligt, wobei der Schwerpunkt auf krisengeschüttelten Regionen liegt.

Aufgrund der Vielschichtigkeit der Einsatzgebiete stellen diese komplexe und vielfältige Sicherheitsherausforderungen dar, die eine gründliche und sorgfältige Risikoanalyse auf strategischer, operativer und taktischer Ebene erfordern. Eine solche Analyse dient als Grundlage für eine angemessene Vorbereitung und wirksame Reaktion auf die vielfältigen Sicherheitsprobleme, die in diesen Einsatzgebieten vorherrschen. In der Tat stellen die Einsatzregionen in der Regel erhebliche Herausforderungen dar, die sich aus verschiedenen ethischen, soziopolitischen, demografischen, (menschen)rechtlichen, ökologischen und technologischen Faktoren ergeben.

Aufgrund des schwierigen Geländes und der oft begrenzten IT-Infrastruktur ist der Einsatz temporärer, transportabler technischer Sicherheitsmaßnahmen unumgänglich. In diesem Zusammenhang erweisen sich offene Quellen (OSINT) als wertvolle Informationsquelle, die ein breites Spektrum von Medien umfassen. Diese Quellen spielen eine entscheidende Rolle bei der Bereitstellung einschlägiger Daten, die für die Überwachung und das Verständnis der dynamischen Entwicklungen in krisengeschüttelten Gebieten unerlässlich sind. Durch die Nutzung offener Quellen, einschließlich lokaler Sensoren, traditioneller Medien und sozialer Medien, wird der rechtzeitige Zugang zu und die gründliche Analyse von relevanten Informationen für die frühzeitige Erkennung von Bedrohungen und die Erstellung eines umfassenden Lagebildes unerlässlich. Es ist jedoch von entscheidender Bedeutung, die Glaubwürdigkeit, Genauigkeit und Herkunft von Informationen aus so unterschiedlichen Quellen und Herausgebern mit Augenmaß zu bewerten. Eine eingehende Prüfung der Datenauthentizität stellt sicher, dass nur zuverlässige und vertrauenswürdige Informationen in die Analyse einfließen, was letztlich zur Effizienz der EU-Missionen angesichts der Sicherheitsherausforderungen beiträgt.

Das Projekt PINPOINT stellt eine Pionierarbeit dar, die sich auf die Entwicklung einer ausgefeilten Methodik konzentriert, die durch einen neuartigen technischen Rahmen ergänzt wird und auf die umfassende Sammlung, Anreicherung und Visualisierung kritischer Daten ausgerichtet ist. Von Bedeutung sind in diesem Zusammenhang die zuverlässigen und präzisen Positions-, Navigations- und Zeitdaten (PNT), die sich auf Personen, Ressourcen, Infrastruktur und andere relevante Elemente beziehen. Diese PNT-Daten dienen als grundlegende Bausteine für die erfolgreiche Durchführung von Missionen im Rahmen der

Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), spielen aber auch eine unverzichtbare Rolle bei der Sicherung und Stärkung lokaler kritischer Infrastrukturen. Die weit verbreitete Anwendung von PNT-Daten erfolgt häufig ohne strenge Prüfung und erfordert proaktive Maßnahmen zur Beseitigung potenzieller Schwachstellen. Die Zugänglichkeit satellitengestützter PNT-Dienste, die auf Plattformen des Globalen Navigationssatellitensystems (GNSS) betrieben werden, hat weiter dazu beigetragen, dass diese Daten oft ungehemmt genutzt werden.

Vor diesem Hintergrund befasst sich das Projekt PINPOINT mit der Erforschung und Entwicklung eines innovativen, transportablen intelligenten Sensorsystems. Dieses System ist auf eine automatisierte PNT-Überwachung zugeschnitten und ermöglicht so eine kontinuierliche und sichere Bestimmung von Position und Zeit. Dieses robuste System ist so konzipiert, dass es potenziellen Manipulationsversuchen standhält, was bei wichtigen Anwendungen wie kritischen Infrastrukturen und GSVP-Missionen einen zusätzlichen Schutz und eine höhere Zuverlässigkeit bietet. Das Projekt schafft einen Rahmen und Instrumente, um diese Faktoren in einer Reihe von Indikatoren zu kombinieren, die eine umfassende und detaillierte Risikoanalyse für solche schwierigen Bedingungen ermöglichen.

Über die reine Technologie hinaus entwickelt und etabliert es jedoch auch eine Methodik, die einen Entwurf für die Anwendung dieser technischen Komponenten, Modelle und Indikatoren liefert. Durch die Erstellung eines mehrdimensionalen Indikatorensatzes soll das daraus resultierende System den österreichischen Nutzern Handlungsoptionen bieten, um flexibel, rasch und adäquat auf sich dynamisch verändernde Einsatzkontexte reagieren zu können. Damit schafft PINPOINT einen greifbaren Nutzen für die Stakeholder in Österreich und trägt zu einer besseren Positionierung innerhalb der EU bei.

Abb.: Österreichische Soldaten liefern im Rahmen einer Friedensmission (EUFOR/ALTHEA) Güter nach Bosnien-Herzegowina

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Austria Institut für Europa- und Sicherheitspolitik (AIES) e.V.
- IGASPIN GmbH
- HENSOLDT Analytics GmbH
- Bundesministerium für europäische und internationale Angelegenheiten
- Bundesministerium für Landesverteidigung

Kontakt:

Martin Boyer
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4284
E-Mail: martin.boyer@ait.ac.at
www.ait.ac.at/

PSH

Einsatz und Ausbildung von Personenspürhunden

Personenspürhunde (PSH) suchen nach dem individuellen Geruch eines Menschen. Aus dem Vergleich mit einem vorher präsentierten Geruchsträger können die Hunde diesen Geruch in ihrem Umfeld finden und dann verfolgen. PSH dienen bei der Polizei der Verfolgung von Straftäterinnen und Straftätern sowie zum Auffinden von vermissten Personen oder ermittlungsrelevanten Beweisen.

Während PSH bei der österreichischen Polizei erst seit 2016 ausgebildet werden, gibt es in Bayern solche Hunde schon seit 2004. Alle Polizeidiensthunde (PDH) werden in Österreich zuerst dual, als Schutz- und Stöberhunde, trainiert und erhalten anschließend eine Spezialausbildung. Besonders begabte Hunde werden als Spezialfährtenhunde trainiert. Bei der Ausbildung zum PSH ist man einen anderen Weg gegangen. Diese Hunde erhalten zuerst ihre Spezialausbildung auf den individuellen Geruch eines Menschen und danach die Grundausbildung als Schutz- und Stöberhund. Bei der bayerischen Polizei werden PSH im Gegensatz zur österreichischen Polizei als reine Spezialisten nur auf den Individualgeruch des Menschen trainiert. Im Rahmen dieses Projekts ergibt sich also die Möglichkeit, nicht nur verschiedene Zugänge und Wege der Ausbildung, sondern auch die Leistungen von Hunden mit unterschiedlichen Einsatzspektren zu vergleichen und Grundlagendaten zum Einsatz von PSH bei der Polizei zu sammeln.

Im Rahmen einer Vergleichsstudie konnten Informationen über das PSH-Wesen bei der Polizei im europäischen Raum gesammelt werden. Als wichtigstes Ergebnis geht daraus hervor, dass Jagd- und Laufhunderassen am häufigsten verwendet werden. Bei der Ausbildung wird ein Spielraum von mehreren Monaten einkalkuliert, da Hunde als Lebewesen auch einen individuellen Leistungsaufbau haben, und es wird eine entsprechende Flexibilität eingeräumt. Zwar gibt es in einigen Ländern ein Konzept oder einen Leitfaden mit vorgesehenen Modulen oder Schritten, diese dienen allerdings nur der Orientierung. Die Zertifizierung für die Einsatzfähigkeit wird unterschiedlich abgewickelt und an den örtlichen Gegebenheiten der zukünftigen Einsatzgefilde sowie an grundlegenden Vorgaben und der Anerkennung vor Gericht ausgerichtet. Nicht nur das Finden der Zielperson, sondern auch das Finden von Gegenständen, die auf diese hinweisen, sowie das Hinführen zu einer entscheidenden Stelle werden als Erfolg des Einsatzes gewertet. Kernelemente für das Gelingen von PSH-Einsätzen bestehen in der Bindung des PSH-Teams, der gegenseitigen Interpretation sowie der Aufrechterhaltung der Motivation für die Tätigkeit und im Willen für die Suche. Ebenso wichtig ist die Offenheit und kreative Gestaltung des Trainings durch die Ausbildnerinnen und Ausbildner. Aus den Informationen dieser Vergleichsstudie wurden weiters Standards für Auswahl, Ausbildung, Zertifizierung und Einsatz von PSH abgeleitet.

Die Trainingsprogramme der österreichischen und der bayerischen Polizei sind in weiten Teilen ähnlich. In manchen Bereichen lehnt sich die Ausbildung der PSH in Österreich stärker an das Training von Fährtenhunden an. Das sieht man auch bei der Überprüfung. In Bayern sind drei Aufgaben zu erfüllen

(negativer Trail am Anfang oder am Ende, Personensuche), wobei die Prüflinge nicht wissen, an welcher Aufgabe gerade gearbeitet werden muss. Im Vergleich dazu haben die Personenspürhundeführerinnen und -führer in Österreich drei Suchen zu absolvieren, die sich nur in Länge, Liegezeit, Untergrund und Anzahl der Gegenstände auf der Fährte unterscheiden.

Bei unseren Experimenten konnten wir zeigen, dass einzelne Hunde Geruchsträger mit einem Altersunterschied von bis zu 64 Wochen miteinander in Verbindung bringen konnten. Nicht nur in einer Laborsituation, sondern auch bei einer einfachen Suche mit wenig Ablenkung waren die Hunde in der Lage, den frischen Referenzgeruch mit einer Geruchsprobe, die bis zu 64 Wochen alt war, zu kombinieren. Unter Realbedingungen war es allerdings so, dass die Hunde im Gelände einen bestimmten menschlichen Geruch schon nach einer Woche nicht mehr finden, geschweige denn ihm folgen konnten. Offensichtlich war hier die Ablenkung durch andere menschliche Gerüche so groß, dass die Hunde bereits nach diesem Zeitraum an ihre Grenzen gestoßen sind.

Nach Analyse von fast 600 Einsatzberichten der PSH in Österreich zeigt sich, dass sich etwa 50 % der Einsätze als erfolgreich bestätigen lassen. Dabei spielt weder der Einsatzzweck noch der Geruchsträger oder das Umfeld eine wesentliche Rolle. Auch die Art und Weise, wie diese Hunde auf die Suche nach bestimmten Personen trainiert wurden, ist sekundär. Wesentlich sind offensichtlich die Einsatzumstände, bei denen die Hunde auf die Strategie zurückgreifen, die sie am schnellsten an ihr Ziel bringt. Dabei verfolgen sie primär den menschlichen Geruch, der ihnen vom Wind zugetragen wird, unabhängig davon, ob sie vorher gelernt haben, einer menschlichen Spur am Boden zu folgen oder sofort mit den leicht flüchtigen Partikeln des menschlichen Geruchs zu arbeiten.

Die im Rahmen des Projekts gewonnenen Erkenntnisse sind einerseits für die Ausbildung von PSH bei der Polizei von großer Bedeutung und fließen unmittelbar in den Ausbildungsbetrieb ein. Andererseits werden PSH auch bei zivilen Rettungsorganisationen zur Suche nach vermissten Personen eingesetzt, und auch diese profitieren von den Ergebnissen dieser Untersuchung.

Abb.: Personenspürhund im Einsatz

Projektleitung:

Universität Salzburg – Ökologie und Evolution

Projektpartner:

- Bayerische Bereitschaftspolizei
- Bundesministerium für Inneres
- Johanniter Österreich Ausbildung und Forschung gem. GmbH

Kontakt:

Dr. Leopold Slotta-Bachmayr
Universität Salzburg
FB Umwelt & Biodiversität
Hellbrunnerstr. 34
5020 Salzburg
Tel: +43 664 282 8667
E-Mail: leopold.slotta-bachmayr@plus.ac.at
www.plus.ac.at/umwelt-und-biodiversitaet/

QKD4GOV

Sicherung von Behördendaten mittels quanten-sicherer Kryptographie

Aufbau eines Behördennetzwerkes zur Erforschung neuer Verschlüsselungsansätze mittels Quantum-Key-Distribution und Post-Quantum-basierter Verschlüsselungstechnologie.

Datensicherheit als Voraussetzung für Datenautonomie ist für die öffentliche Hand und kritische Infrastrukturen eine grundlegende Notwendigkeit, um die ökonomische Wettbewerbsfähigkeit ebenso wie eine selbstständig agierende nationalstaatliche Sicherheit nachhaltig zu gewährleisten. Die Sicherung von vertraulichen Daten, Datenintegrität und Datenherkunft durch aktuelle Verschlüsselungsverfahren ist aber durch die globalen Entwicklungen und Investitionen in Quantencomputer grundlegend bedroht, da heute verwendete asymmetrische Verschlüsselungsverfahren (Public-Key-Kryptographie) dadurch gebrochen werden können. Somit ist es notwendig, neue Verschlüsselungstechnologien und -systeme zu entwickeln, welche „quantum-safe" sind. Dabei gibt es 2 mögliche Ansätze, einerseits können klassische Verfahren gegen Quantencomputer-Attacken gestärkt werden, man spricht dann von „Post-Quantum-Kryptographie" (PQC), oder es können Quantenkommunikations-Algorithmen eingesetzt werden, meist Quantenschlüsselverteilung (QKD), die gegen jegliche Attacke sicher sind.

Österreich und im Speziellen das Austrian Institute of Technology (AIT) haben auf beiden Forschungsgebieten eine international führende Rolle eingenommen und mit nationalen Partnern das geförderte Projekt QKD4GOV ins Leben gerufen. Als Bedarfsträger standen dafür das Bundeskanzleramt Österreich (BKA), Bundesministerium für europäische und internationale Angelegenheiten (BMeiA), Bundesministerium für Landesverteidigung (BMLV) und Bundesministerium für Inneres (BMI) zur Verfügung. Ziel von QKD4GOV war es, modernste Verschlüsselungstechnologien basierend auf QKD als auch Post-Quantum-Kryptographie für eine zukünftige hochsichere Kommunikationsinfrastruktur der Österreichischen Bundesministerien und Behörden zu erforschen. Zu Beginn des Projektes wurden, zusammen mit den Bedarfsträgern und zwei österreichischen Firmen (fragmentiX Storage Solutions und X-Net), zwei Anwendungsfälle konzipiert, um die technologische Reife von Quantenschlüsselverteilung im realen Einsatz zu demonstrieren. Um einen Know-how-Transfer dieser Technologien zu beschleunigen, wurden die Bedarfsträger direkt in die Demonstrationen eingebunden. Hierfür wurde vom Projektpartner CableRunner ein innerstädtisches Glasfasernetz in Wien aufgebaut, das das Bundeskanzleramt sowie die Bundesministerien BMLV, BMI verband. Die QKD-Geräte sowie Link-Encryptoren wurden direkt in den Serverräumen der Bedarfsträger installiert, um so die Kommunikationsverbindungen zwischen den Ministerien zu sichern.

Ziel des ersten Anwendungsfalls war es, wie mit den Methoden der Quantenkryptographie und des Secret Sharings die Übertragung, Speicherung und die kontrollierte gemeinsame Nutzung von klassifizierten Dokumenten in Zukunft ermöglicht werden kann. In einer Proof-of-Concept-Demonstration stellte die Firma fragmentiX Storage Solutions ihre Secret-Sharing-Technologie zur Verfügung, die es ermöglicht,

Daten in Paketen aufzuteilen und diese Teile an separaten Orten zu speichern. Nur wenn alle Teile wieder zusammengeführt werden, ist eine Rekonstruktion des originalen Datensatzes möglich. Kombiniert mit dem QKD-Netzwerk, konnte gezeigt werden, dass Behördendaten sowohl abhörsicher übertragen als auch abgespeichert werden könnten. Im zweiten Anwendungsfall ging es um die Sicherung der direkten Kommunikation zwischen den Bedarfsträgern mittels einer modifizierten Chat-Anwendung, die von AIT und der Firma X-Net implementiert wurde. Bei der Übertragung wurde jede einzelne Nachricht mit PQC-Methoden abhörsicher verschlüsselt und authentifiziert sowie für die Übertragung zwischen verschiedenen Standorten mit von QKD-Geräten erzeugten Schlüsseln zusätzlich abgesichert. Wie im Fall des Secret Sharings wurde auch diese Anwendung im aufgebauten QKD-Netzwerk gezeigt. Des Weiteren wurde im Rahmen einer Technologieweiterentwicklung das Konzept der hybriden Schlüsselverteilung erforscht. Dabei wird Schlüsselmaterial von QKD und PQC derart zusammengefügt, dass selbst bei Ausfall einer der Komponenten das System sicher bleibt. Mehr noch, eine Ende-zu-Ende-Authentifizierung in großen quantensicheren Netzwerken (wie in dem unten erwähnten Euro-QCI) kann dadurch ebenfalls erreicht werden. Die enge Kooperation zwischen den öffentlichen Bedarfsträgern und österreichischen Unternehmen stellt die Verankerung der behördlichen Bedürfnisse aus Sicht des IT-Endnutzers sowie der Sicherheitsanforderungen in der Entwicklung der QKD-Sicherheitstechnologie sicher. Neben den technologischen Forschungsergebnissen sind die Resultate aus QKD4GOV auch die Grundlage für die Positionierung Österreichs und dessen aktive Gestaltung in der europäischen EuroQCI-Initiative und liefern ebenso die Basis für eine zukünftige nationale Kryptoinfrastruktur für Behörden.

Die von der Europäischen Kommission gestartete Initiative „EuroQCI – Quantum Communication Infrastructure“ hat zum Ziel, ein quantengesichertes Kommunikationsnetzwerk für klassifizierte Daten in den nächsten 10 Jahren mithilfe aller Mitgliedsstaaten in Europa zu errichten.

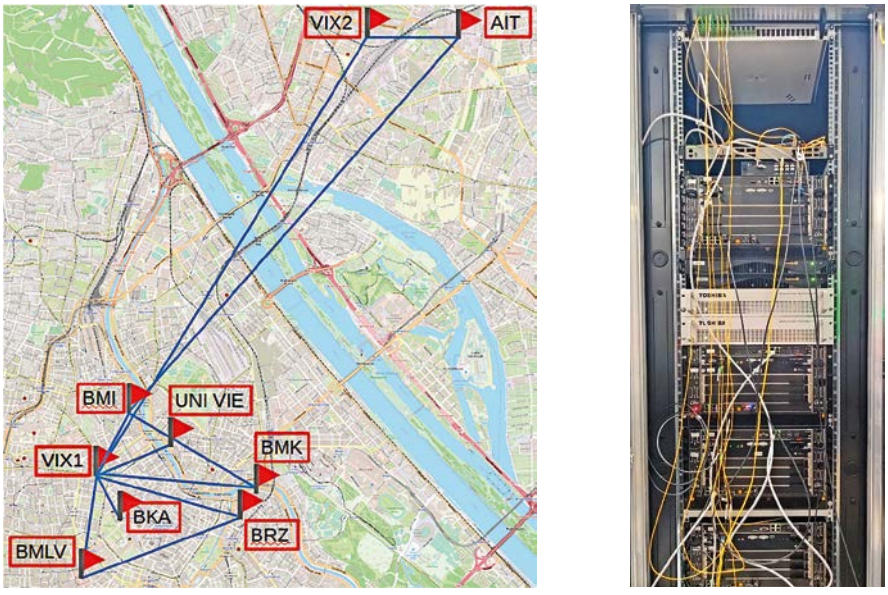


Abb.: Plan des QKD-Netzwerks in Wien, in dem die QKD4GOV-Demonstrationen durchgeführt wurden; links: typischer Aufbau eines QKD-Knotens in einem Serverraum

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- fragmentiX Storage Solutions GmbH
- X-Net Services GmbH
- CableRunner Austria GmbH & Co. KG
- Universität Wien – Institut für Europarecht
- Bundeskanzleramt Österreich (Bedarfsträger)
- Bundesministerium für europäische und internationale Angelegenheiten (Bedarfsträger)
- Bundesministerium für Landesverteidigung (assoz. Bedarfsträger)
- Bundesministerium für Inneres (assoz. Bedarfsträger)

Kontakt:

Dr. Hannes Hübel
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4453
E-Mail: hannes.huebel@ait.ac.at
www.ait.ac.at/

ReaGtSion

Resilienzbedarfsermittlung von Gütern und Services österreichischer Schlüsselindustrien

Die Covid-19-Krise hat deutlich punktuelle Schwächen in den wirtschaftlichen Versorgungsnetzwerken aufgezeigt. Im Hinblick auf eine resiliente Gesellschaft und auf ein nationales Kontinuitätsmanagement müssen Lieferunterbrechungen und Versorgungsengpässe frühzeitig erkennbar sein, um ihnen auch aktiv entgegenwirken zu können. Dabei genügt es nicht, nur die klassischen kritischen Infrastrukturen zu betrachten, sondern es ist auch notwendig, den Fokus auf Schlüsselindustrien zu verbreitern. So können sie etwa als Zulieferer von wichtigen Vor- oder Zwischenprodukten, Unterstützungsleistungen (Reparaturservices etc.) oder Know-how auftreten.

Ein Hauptziel des Projekts ReaGtSion ist die Definition eines strukturierten, aber generischen Vorgehensmodells, welches die Erfassung der kritischen Komponenten (Unternehmen und den Abhängigkeiten dazwischen) unterstützt und eine Analyse von möglichen Schwachstellen erlaubt. Hierbei waren vor allem die Ausrichtung der Analyse (prozess- und ablauforientiert) sowie die Detailtiefe (high-level und abstrahiert) der zu modellierenden Systeme ausschlaggebend. Um die inhaltlichen Diskussionen zu konkretisieren, wurden fünf Use-Case-Szenarien identifiziert, die Wertschöpfungsnetzwerke aus unterschiedlichen Bereichen betrachten: Erdgas (Kritikalität aufgrund des Ukraine-Russland-Krieges), Dünger (als Nebenprodukt der Erdgas-Raffinierung), Halbleiter (Fokus auf globale Lieferketten), Kobalt (repräsentativ für die Verwendung bei erneuerbaren Energien) und Haushaltsbatterien (im Hinblick auf Stromausfälle).

Die Analysen liefern einen Überblick über mögliche Vulnerabilitäten und Risiken in den jeweiligen Wertschöpfungsketten, etwa Einzelquellbeschaffung („Monoketten"), Abhängigkeiten von dominierenden Lieferpartnern, Lieferwegen, orthogonale Einflussfaktoren – wie z. B. Verfügbarkeit von Fachpersonal oder rechtliche Rahmenbedingungen –, aber auch zeitliche Aspekte. Auf Basis der aus den einzelnen Use Cases erhaltenen Informationen und Daten wurden die Wertschöpfungsnetzwerke für alle fünf Bereiche aufgebaut, wobei das Netzwerk für Erdgas in einem höheren Detail erstellt werden konnte, da durch die Kritikalität vermehrt Informationen bereitgestellt wurden. Für die weitere Analyse wurde daher der Use Case Erdgas herangezogen. Die erhobenen Informationen flossen in ein Simulations-Tool ein, das bereits durch den Projektpartner AIT entwickelt wurde. Darin wurden die wichtigen Standorte der Gasversorgung und -speicherung in Österreich modelliert und geografisch verortet; die Verbindungen zwischen den Standorten stellen dabei die Versorgungsleitungen dar. Aufgrund der Komplexität wurden die Erdgasleitungen jedoch eher schematisch eingefügt (ohne ebenfalls geografisch verortet zu werden) und einzelne größere und kleinere Abnehmer beispielhalft eingefügt.

Time	Entity Name	Event	New State	Because Of
10	(Mitglied der Heizel Group)	Erdgasknappheit	2	Portschach 6
10	Arnoldstein	Erdgasknappheit	3	Finkenstein am Faaker See
10	Marcher Villach	Erdgasknappheit	3	Finkenstein am Faaker See
10	Veitsch-Radex (Bergbau)_Radentheln	Erdgasknappheit	4	Finkenstein am Faaker See
11	Finkenstein am Faaker See	Erdgasknappheit	3	Ebenthal 856/1
11	Marcher Klagenfurt	Erdgasknappheit	1	Ebenthal 856/1
12	Arnoldstein	Erdgasknappheit	4	Finkenstein am Faaker See
12	Marcher Villach	Erdgasknappheit	3	Finkenstein am Faaker See
12	Veitsch-Radex (Bergbau)_Radentheln	Erdgasknappheit	4	Finkenstein am Faaker See

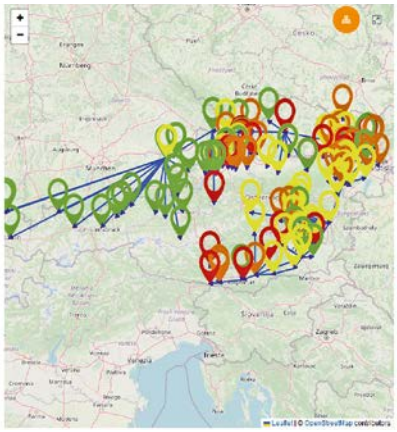


Abb.: Ergebnisse aus der Simulation des Szenarios zur Erdgasknappheit

Mit diesem Modell wurde daraufhin eine Erdgasknappheit simuliert. Angenommen wurde dabei eine Mangellage im Ausland (ohne konkrete Angabe eines Auslösers), wodurch es zu einer Unterversorgung am Einspeisungspunkt in das österreichische Netzwerk kommt. Mit Hilfe des Simulationstools konnten die Kaskadeneffekte, die sich durch diese Unterversorgung ergeben, im gesamten Netzwerk dargestellt werden. Aufgrund der stochastischen Natur der Analyse wurde eine Reihe von Simulationen durchgeführt, und die Ergebnisse wurden daraufhin statistisch ausgewertet, um einen Überblick zu bekommen, welche die am stärksten betroffenen Knoten im Wertschöpfungsnetzwerk sind, welche Knoten (aufgrund der Anzahl ihrer Verbindungen) als besonders kritisch für die Versorgung eingestuft werden können und welche Punkte als neuralgisch im gesamten Netzwerk einzustufen sind.

Zur Validierung der Analysemethoden und Ergebnisse wurde unter Einbindung der Expertinnen und Experten der Bedarfsträger eine Krisenübung veranstaltet. Hierfür wurde die Versorgung mit Milchprodukten gewählt. Als Ausgangslage wurde ein Blackout angenommen, der bereits seit 72 Stunden andauert und ganz Mitteleuropa betrifft. Die Fragestellung der Übung betraf die vorbereitenden Prozesse für ein Wiederanlaufen der Produktion in den Betrieben sowie die Betrachtung der damit verbundenen weiteren Liefer- und Versorgungsketten sowie orthogonaler Faktoren wie Transport, Verkehr und Kommunikation (Kaskadeneffekte). Im Rahmen der Übung wurde auch die Simulationskomponente vorgestellt. Ziel war es dabei, das direkte Feedback der übenden Personen in die Simulationsumgebung einzubringen und dadurch die potenziellen Kaskadeneffekte darstellen zu können.

Auf Basis der Analyseergebnisse wurden gemeinsam mit den Bedarfsträgern potenzielle Maßnahmensetzungen evaluiert und daraus neun zentrale Handlungsoptionen auf wirtschaftspolitischer und sicherheitspolitischer Ebene erarbeitet, die sich von der Schaffung einer gemeinsamen Datenbasis in Österreich bis hin zum Aufbau eines Krisenstabs innerhalb des BMAW sowie eines CERTs für den Versorgungsbereich auf österreichischer Ebene erstrecken, um die Resilienz von Wertschöpfungsketten zu steigern.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Bundesministerium für Digitalisierung und Wirtschaftsstandort
- Bundesministerium für Inneres
- FH OÖ Forschungs & Entwicklungs GmbH
- INFRAPROTECT Gesellschaft für Risikoanalyse, Notfall- und Krisenmanagement GmbH
- Mar Adentro e.U
- Wirtschaftskammer Österreich

Kontakt:

Dr. Stefan Schauer
AIT Austrian Institute of Technology GmbH
Lakeside B10a
9020 Klagenfurt am Wörthersee
Tel: +43 664 825 14 55
E-Mail: stefan.schauer@ait.ac.at
www.ait.ac.at

RESIST

Digitales Pandemie- und Krisenmanagement in der Trinkwasserversorgung

Die urbane Trinkwasserversorgung gewährleistet eine zuverlässige Versorgung der Bevölkerung mit Trinkwasser in ausreichender Menge und Qualität und stellt somit einen wesentlichen Bestandteil der städtischen Infrastruktur dar. In Österreich gibt es rund 5.500 Wasserversorgungsunternehmen (WVU), wobei der Großteil der Bevölkerung durch kleine (Genossenschaften, Verbände, Gemeinden) und mittlere (städtische) WVU mit Trinkwasser versorgt wird.

Ausgangsbeschränkungen wie im Frühjahr 2020 stellten auch WVU vor neue Herausforderungen. Dazu gehören markante räumliche und zeitliche Veränderungen des Wasserbedarfs im Versorgungsnetz, ausgeprägte Frühjahrstrockenheit, Umstellung auf Notbetrieb, Personalmanagement und Quarantänemaßnahmen. Besonders kleine WVU waren betroffen. Die fortschreitende Digitalisierung im Bereich Trinkwasserversorgung (z. B. digitale Wasserzähler, Druck- und Qualitätssensoren) ermöglicht jedoch eine kontinuierliche Überwachung und Steuerung der Systemzustände, wodurch innovative Ansätze für das zukünftige Pandemie- und Krisenmanagement entwickelt werden können.

Integrative Resilienzbetrachtungen von Wasserversorgungssystemen (Digitalisierung als Krisenwerkzeug, aber auch zusätzliches Gefährdungspotenzial durch vielfältige Zugriffspunkte) finden in der Praxis und in der Literatur noch wenig Beachtung.

Ziel des Forschungsprojektes RESIST ist es daher, das Krisen- und Pandemiemanagement der Trinkwasserversorgung, insbesondere bei kleinen und mittleren WVU, im Zusammenhang mit der digitalen Transformation zu verbessern.

Zu Projektbeginn wurde der Vorbereitungsstatus der WVU in Österreich erhoben. Hierfür wurde eine Umfrage über die Erfahrungen und gesetzten Maßnahmen in den „Pandemiejahren“ 2020 bis 2022 an die österreichischen WVU zur Beantwortung versendet. Die Umfrage umfasste 27 Fragen zu unterschiedlichsten Themenbereichen und wurde von insgesamt 71 WVU beantwortet. Dadurch konnten verschiedenste Ansätze und Lösungen erhoben werden, welche anschließend von den Praxispartnern für die Aufbereitung von Best-Practice-Anleitungen zur Pandemiebewältigung oder Ähnlichem genutzt wurden.

Im zweiten Projektabschnitt erfolgt eine modellbasierte Untersuchung der Verletzlichkeit bestehender Infrastruktur gegenüber Störfällen. Hierfür wurde eine Literaturstudie durchgeführt, in der verschiedene mögliche Störfälle identifiziert wurden. Im Zuge der Pandemie wurden zusätzlich neuartige Störfälle wie Ausgangsbeschränkungen mit Verbrauchsänderungen oder Wissensverlust durch Personalwechsel (Quarantäne, Generationswechsel) identifiziert. Des Weiteren wurden neuartige, Graphen-basierte Ansätze aus der Grundlagenforschung an die spezifischen praxisrelevanten Bedingungen der alpinen Fallstudie WVU Schwaz angepasst und erprobt. Die kürzeren Analysezeiten ermöglichen eine größere Tiefe von „Was-wäre-wenn“-Untersuchungen zur effizienteren Identifikation von Schwachstellen. Zudem

werden auch störfallübergreifende Szenarien, z. B. Ausgangsbeschränkung und cyber-physischer Angriff, systematisch untersucht und Verbesserungspotenziale aufgezeigt.

Aufbauend darauf werden die identifizierten Schwachstellen mit verschiedenen Maßnahmen proaktiv adressiert. Neben technischen (z. B. neue Leitungen) und digitalen (z. B. Frühwarnsysteme) Ansätzen ist dabei die Berücksichtigung von sozio-technischen Aspekten wesentlich, da die Auslastung der Versorgungsnetzwerke während Krisen auch stark vom jeweiligen Benutzerverhalten abhängig ist. Beispielsweise kann eine unkoordinierte Entnahme von Trinkwasser für Vorratszwecke oder Ähnliches zu kurzfristigen Beeinträchtigungen führen. Daher werden im Projekt auch verschiedene Strategien zur Krisenkommunikation aus soziologischer Sicht untersucht, um den Betreibern von WVU wichtige Erkenntnisse im Umgang mit der Bevölkerung während Krisenzeiten zu liefern.

Die Ergebnisse zur Steigerung der Resilienz durch technische, sozio-technische und digitale Ansätze während Störfallen werden anschließend von Juristinnen und Juristen bezüglich der rechtlichen Umsetzbarkeit bewertet und von den Praxispartnern für die Erstellung von Handlungsempfehlungen und Handbüchern (z. B. in Form von Best-Practice-Anwendungen und Checklisten) verwendet. Durch die praxistaugliche Umsetzung steht den WVU und Behörden eine umfangreiche Literatur für das Krisenmanagement zur Verfügung. Zudem wird an einer Open-Source-Plattform für die (Echtzeit-)Simulation und Visualisierung von ausgewählten Störfällen gearbeitet, um die Übertragbarkeit auf andere Fallstudien zu unterstützen.

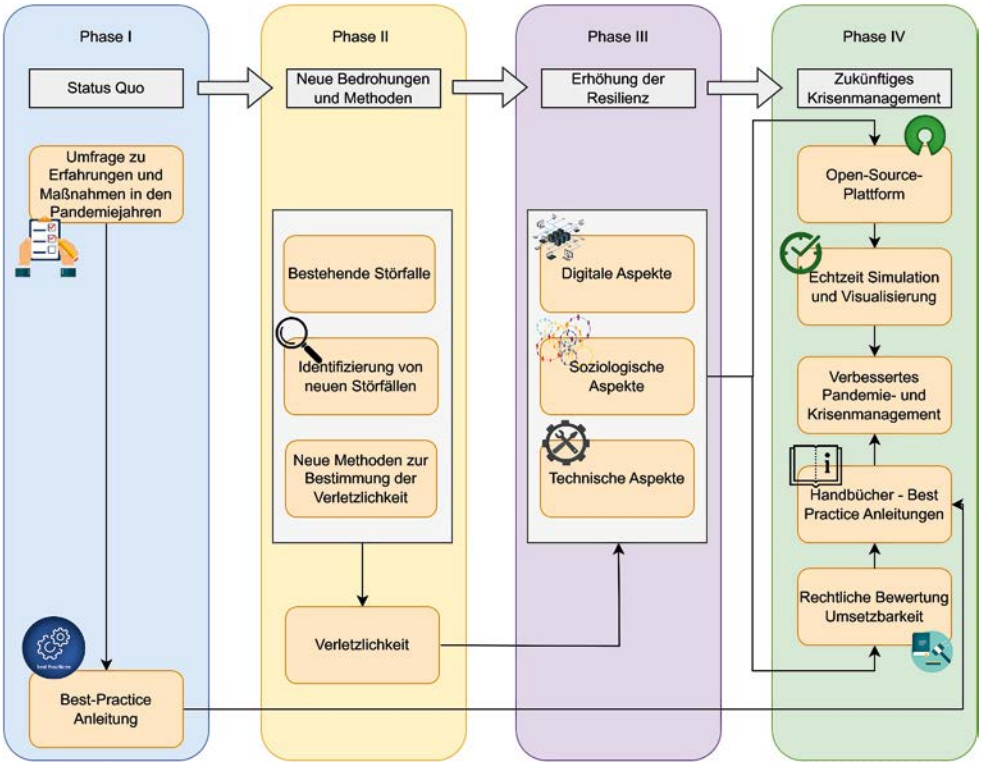


Abb.: Übersicht über das Forschungsprojekt „RESIST“

Projektleitung:

Universität Innsbruck

Projektpartner:

- Österreichische Vereinigung für das Gas- und Wasserfach
- Stadtwerke Schwaz GmbH
- Universität Innsbruck – Institut für Öffentliches Recht, Staats- und Verwaltungslehre
- Universität Innsbruck Institut für Soziologie
- Wasser Tirol – Dienstleistungs-GmbH
- ZetaLabs IT-Service

Kontakt:

Univ.-Prof. Dipl.-Ing. Dr. techn. Robert Sitzenfrei
Universität Innsbruck
Technikerstr. 13
6020 Innsbruck
Tel: +43 512 507 62195
E-Mail: Robert.Sitzenfrei@uibk.ac.at
www.uibk.ac.at

RIFIDAS

Rapid In-Field Identification of Addictive Substances

Drogenmissbrauch ist ein Problem, und zwar nicht nur für die Konsumentinnen und Konsumenten, sondern auch für viele andere Bereiche der Gesellschaft. Auch die Exekutive ist mit der Bearbeitung von Suchtmittelfällen personell und finanziell stark belastet. In Verdachtsfällen, z. B. im Rahmen von Streifeneinsätzen oder Routinekontrollen, muss in vielen Fällen mit hohem administrativen Aufwand eine Laboranalyse der verdächtigen Substanzen veranlasst werden. Und bei einem nicht unerheblichen Anteil dieser Analysen stellt sich dann heraus, dass das beanstandete Material tatsächlich legal im CBD-Shop erworbenes Cannabis war.

Ein verlässliches, einfach zu handhabendes Vortestgerät in der Hand von Exekutivbeamten wird helfen, bereits am Beginn der Amtshandlung zu klären, ob mit hoher Wahrscheinlichkeit ein Suchtmitteldelikt vorliegt oder nicht. Somit werden erhebliche Ressourceneinsparungen ermöglicht. Darüber hinaus werden unbegründete Fälle von Probensicherstellungen oder gar von Freiheitsentzug in Zusammenhang mit vermeintlichem Suchmittelbesitz wesentlich reduziert, was sich positiv auf soziale und rechtliche Belange auswirkt. Exakt ein solches schnell und einfach einsetzbares Vortestgerät für die Exekutive wird im Rahmen von RIFIDAS entwickelt.

Legales oder illegales Cannabis

Durch das zunehmende Aufkommen von legalem CBD-Cannabis verschärft sich die Belastungssituation für die Exekutive mehr und mehr, da es derzeit keine zuverlässige Methode für Exekutivbeamte gibt, um schnell und sicher vor Ort zwischen legalen und illegalen Substanzen zu unterscheiden. Von legalem CBD-Cannabis spricht man bei Substanzen mit einem Gehalt von < 0,3 % THC (in den getrockneten Blütenbestandteilen). Das Problem ist, dass diese Produkte visuell und olfaktorisch nicht von dem durch das Suchtmittelgesetz kontrollierten hoch THC-haltigen Cannabis unterscheidbar sind.

Um diesen Bedarf an einer schnellen, zuverlässigen, mobilen und robusten Messtechnik zur Vorklassifizierung im Rahmen von routinemäßigen Amtshandlungen der Exekutive zu decken, ist speziell Spektroskopie im nahen Infrarotbereich (NIR) interessant, da sich hier aufgrund neuester Entwicklungen im Bereich Mikro-Opto-Elektro-Mechanischer-Systeme (MOEMS) äußerst kostengünstige und flexible Messansätze realisieren lassen.

Der technische Lösungsansatz

Bereits erhältliche NIR-Messlösungen zur THC-Messung sind für die betrachtete Anwendung jedoch aus verschiedenen Gründen ungeeignet: zu hoher Preis, notwendige Probenvorbereitung, Unhandlichkeit, für Einsatzkräfte z. B. aus Datenschutzgründen nicht anwendbare Systemkonzepte.

Unter der Leitung der oberösterreichischen Forschungseinrichtung RECENDT wurde daher ein Konsortium gemeinsam mit dem Bedarfsträger (BMI) gebildet, um mit der Expertise in spektroskopischer Sensortechnik (RECENDT) und Elektronikdesign (HW/SW, Partner MEDS) auszuloten, wie ein völlig neuartiges Gerätekonzept entwickelt werden kann. Der GSK-Partner VICESSE sorgt dafür, dass das gesamte Messkonzept allen juristischen Anforderungen für den späteren Praxiseinsatz genügt.

Der Fokus wurde im Projekt ausschließlich auf die Unterscheidung zwischen legalem und illegalem Cannabis gelegt, da dies mit 60–70 % Anteil an den Gesamtanzeigen nach dem Suchtmittelgesetz zurzeit die größte Belastung darstellt.

In der ersten Entwicklungsphase wurde eine Auswahl aus den zur Verfügung stehenden grundlegenden aktuellen Spektrometertechnologien (basierend z. B. auf Digital Light Processing sowie Solid-State-Technologie) getroffen und das grundlegende Messkonzept im Labor erarbeitet. Dieses musste nun noch in ein Hand-Messgerät übergeführt werden. Dazu wurde ein Gerätedesign entwickelt und die nötige Hardware konstruiert und in einigen Zyklen mithilfe von 3-D-Druck-Prototypen optimiert. Parallel wurde die nötige Elektronik und Software entwickelt und alle Komponenten zu einem Funktionsmuster zusammengeführt.

In der letzten (und zu Redaktionsschluss dieses Beitrags noch laufenden) Projektphase werden einige Exemplare dieser Funktionsmuster durch Exekutivbeamtinnen und -beamten im Feldeinsatz erprobt. Aus den Erkenntnissen wird eine sogenannte Road to market für die Produktüberleitung erstellt.

Road to market

Die Ergebnisse des Entwicklungsprojektes von einem Kommerzialisierungspartner aufgegriffen werden. Um die Kommerzialisierung der entwickelten Lösung abzusichern, wurde bereits ein entsprechendes Patent eingereicht. Mit verschiedenen interessierten österreichischen Partnern laufen vertrauliche Gespräche, um Lizenz- und Verwertungsverträge für die Produktüberleitung zu erzielen. Aus dem Funktionsmuster soll noch 2024 ein Produkt werden, das die polizeiliche Arbeit erleichtert. Der Markt für ein derartiges Produkt ist nicht auf die Ausstattung der österreichischen Polizei beschränkt. Einerseits ist das entwickelte Vortestgerät für Polizeikräfte weltweit einsetzbar, andererseits basiert die entwickelte Lösung auf einem flexiblen Ansatz und kann später durch Anpassung der chemometrischen Modelle mit wenig Aufwand auf andere Suchtmittel oder andere Einsatzfelder erweitert bzw. adaptiert werden.

Abb.: Ein erster Entwicklungsprototyp im Test, die Daten werden am Smartphone weiterverarbeitet

Projektleitung:

RECENDT – Research Center for Non-Destructive Testing GmbH

Projektpartner:

- Bundesministerium für Inneres (Bedarfsträger)
- MEDS (Spath Micro Electronic Design GmbH)
- VICESSE (Vienna Centre for Societal Security), Wien

Kontakt:

Robert Holzer
RECENDT – Research Center for Non-Destructive Testing GmbH
Altenberger Straße 69, Science Park 2 / 2. OG
4040 Linz
Tel: +43 732 2468 4602
E-Mail: robert.holzer@recendt.at
www.recendt.at

RIO

Resilienz im Onlinehandel

Die Anwendung von KI als Beitrag in der Betrugserkennung und der technisch gestützten Präventivarbeit ist nicht nur vielversprechend, sondern zu einer unabdingbaren Notwendigkeit geworden, denn Onlinebetrug ist schwieriger zu erkennen und es bleibt wenig Zeit dafür: Fake-Shops werden massenhaft ausgerollt, erzielen über Werbung eine hohe Effektivität in der Zielgruppenerreichung und verschwinden nach kurzer Zeit wieder. Im Jahr 2021 kam es mit 18.780 Anzeigen (+19,5 %) zu einem erneuten Höchststand, Studien beziffern den direkten Schaden auf 16 Millionen Euro und rechnen mit 320.000 betroffenen Konsumentinnen und Konsumenten in Österreich. Entsprechend haben zentrale Stakeholder wie die Europäische Kommission die Notwendigkeit für neue, technisch gestützte Präventivsysteme erkannt, die Behörden bei ihrer Arbeit unterstützen sollen.

Der Einsatz von KI ermöglicht eine zusätzliche und wertvolle „Sichtweise" für Expertinnen und Experten, denn auch wenn Seiten optisch gänzlich unterschiedlich aussehen, so hinterlassen Täter Fingerabdrücke im Code, die durch die KI gefunden werden. Dies ist durch den Umstand begründet, dass dem Bestellbetrug „Crime as a Service" die Verwendung von Drittdienstleistern oder der Ursprung in organisierten internationalen Täter-Gruppen zugrunde liegt.

Als Kern-Innovation des KIRAS-Projekts SINBAD wurde durch die Konsortialpartner AIT, ÖIAT und XNET ein technisch gestütztes Präventivsystem zum Echtzeitschutz für Konsumentinnen und Konsumenten entwickelt, welches in der Lage ist, Fake-Shops von seriösen Angeboten aufgrund der Ähnlichkeit zu bereits bekannten betrügerischen Angeboten auf über 21.000 Merkmalsräumen zu unterscheiden. Die Stärke des Verfahrens liegt darin begründet, dass kein einzelnes Merkmal, sondern die Kombination einer Vielzahl von Einzelmerkmalen, und hierbei ihr Vorhandensein oder Nicht-Vorhandensein, zu einer sehr robusten Risikobewertung durch die KI führt. Das Projekt resultierte in der Inbetriebnahme des Fake-Shop Detectors (FSD), der kostenlos über die Browser-Plugin-Stores von Firefox, Chrome und Edge verfügbar ist, täglich von über 8.000 Nutzerinnen und Nutzern verwendet wird und im Praxiseinsatz bei 1,2 Millionen Domains und über 5,3 Millionen Risikobewertungen der KI eine Genauigkeit von 88 % erzielt. Die Wirkungsweise von FSD in der Reduktion des Window of Opportunity von betrügerischen Online-Angeboten wurde 2022 im Screening von neu registrierten Domains in Österreich erfolgreich gezeigt, indem ein geschätzter volkswirtschaftlicher Schaden von 628.500 € abgewehrt werden konnte.

Abb.: Fake-Shop Detector in a nutshell

Das Projekt Resilienz im Online-Handel (RIO), gefördert aus Mitteln des österreichischen Sicherheitsforschungsprogramms KIRAS in der Ausschreibung 2021, setzt die erfolgreiche technisch gestützte Präventionsarbeit gegen Betrug im Onlinehandel durch zielgerichtete Innovationen entlang des Fake-Shop-Detection-Lifecycles fort. Die Kernziele von RIO umfassen u. a. die Entwicklung und Bereitstellung einer modular skalierbaren und einfach erweiterbaren Open-Source-Plattform für KI-basierte Risk-Assessment-Services und deren Anwendungen im Praxiseinsatz. Ein weiterer Schwerpunkt ist die Adressierung von Betrugsprävention auf Online-Marktplätzen durch Methoden des Natural Language Processing (NLP) mit dem Ziel zur Steigerung der menschlichen Nachvollziehbarkeit KI-basierter Risiko-Bewertungen sowie die Entwicklung von Demonstratoren zur Auffindung und Exponierung zusammenhängender Betrugsfälle (Fake-Shop Cluster) unter Begleitung der Bedarfsträger BMI und BMSGPK, inklusive einer Evaluierung des Einsatzpotenzials hinsichtlich ihrer ergänzenden Wirkung in der Präventionsarbeit und Kriminalitätsbekämpfung. Annähernd jeder siebte Euro, der für Haushaltsausgaben zur Verfügung steht, wurde 2021 für Waren im E-Commerce ausgegeben. Der Brutto-Umsatz mit Waren im deutschen E-Commerce betrug 2021 99,1 Milliarden Euro (+19 % zu Vorjahr), dabei wurden 40,2 Prozent des Umsatzes über mobile Endgeräte erwirtschaftet. Über Online-Marktplätze wird mehr als jeder zweite Euro umgesetzt. Doch gerade auf mobilen Geräten sind Konsumentinnen und Konsumenten deutlich vulnerabler. Diesem Umstand wird in RIO durch einen Mobile-first-Ansatz sowie die Umsetzung einer minimalinvasiven App-Lösung für den mobilen Echtzeitschutz vor Betrugsfallen Rechnung getragen. Durch die Integration des Fake-Shop Detectors in die Abläufe der Watchlist Internet, der größten deutschsprachigen Meldestelle für Internetbetrug, erreichte die Anzahl der veröffentlichten Warnmeldungen einen neuen Höchststand. Hierbei gilt es, Expertinnen und Experten durch die Entwicklung eines community-enabled Fraud-Präventionsansatzes zu entlasten, indem Aufgaben der KI-Qualitätssicherung durch geeignete Gamification- und Nudging-Ansätze an die Community delegiert und automatisiert sowie identifizierte Seiten durch eine Fake-Shop-Traffic-Impact-Analyse von Mobile-Network-Monitoring-Daten begleitet werden. Neben dem Schwerpunkt der Fake-Shop-Prävention wird in RIO die Ausweitung des erfolgreichen FSD-Ansatzes auf andere Anwendungsfelder, als Proof-of-Concept, im Bereich der Warnung vor betrügerischen Kryptowährung-Investmentplattformen erprobt.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- cyan Security Group GmbH
- Österreichisches Institut für angewandte Telekommunikation
- Bundesministerium für Inneres
- Bundeskriminalamt
- Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz, Sektion Konsumentenpolitik und Verbrauchergesundheit (Bedarfsträger)
- Bundesministerium für Inneres (Bedarfsträger)
- X-Net Services GmbH
- Xylem – Science and Technology Management GmbH

Kontakt:

Mag. Andrew Lindley
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 664 815 7848
E-Mail: andrew.lindley@ait.ac.at
www.ait.ac.at

ROADS to Health

Entscheidungsunterstützung für das Pandemiemanagement der Zukunft

Covid-19 hat zur weltweit größten von einem Virus verursachten Krise der letzten Jahrzehnte geführt. Wie viele andere Staaten war auch Österreich in einigen Bereichen unzureichend auf eine Pandemie vorbereitet. Das Pandemiemanagement war deshalb in den meisten Hinsichten reaktiv anstelle von präventiv ausgerichtet. Dies führte für die Bevölkerung zu teilweise schwer nachvollziehbaren Maßnahmensetzungen. Um dieser Problematik in Zukunft besser entgegentreten zu können, zielt ROADS darauf ab, Bedarf und Grundlagen für ein evidenzbasiertes Maßnahmen-Matching im Pandemiefall auszuarbeiten. Dabei wird ein technologisches Konzept (Tool) erstellt, das jeweilige Schritte im Pandemiemanagement vorschlägt, um Maßnahmen an die gegebene Situation und voraussichtliche Szenarien anzupassen.
Mittels technischer Systeme können Entscheidungen im Pandemiemanagement schneller und fundierter getroffen werden. Zum einen hat das richtige Timing von Maßnahmensetzungen unmittelbare Auswirkungen auf den weiteren Pandemieverlauf. Zum anderen helfen evidenzbasierte Entscheidungsvorgaben, dass Maßnahmen in gezielten Bereichen die gewünschten Auswirkungen haben. Das Maßnahmen-Matching als Entscheidungsunterstützung im ROADS-Projekt soll auf die bestehende Rahmenplattform „Portfolio of Solutions“ (POS) aufgesetzt werden. Die POS-Plattform ermöglicht mittels semiautomatisierter Verknüpfungen nutzerfreundliche, übersichtliche Dashboard-Darstellungen für zielgerichtete und bedarfsgerechte Analysen, Modelle und Entscheidungen. Der Innovationsgehalt des Projektes beruht auf den Erkenntnissen aus der Covid-19-Krise und ergibt sich aus der Zusammenführung praktischer Erfahrungen aus dem Krisenmanagement, dem Bedarf kritischer Infrastrukturen sowie wissenschaftlicher Erkenntnisse und Studien. ROADS soll dadurch zukünftige Pandemiebewältigung unter Rücksichtnahme einer gesamtgesellschaftlichen Perspektive unterstützen. Dabei wurden alle Faktoren, die in die Entwicklung des Tools einfließen und den inhaltlichen Rahmen für Entscheidungen im Pandemiemanagement bieten sollen, berücksichtigt. Letztlich können Entscheidungsträger Maßnahmen setzen, die Zielsetzungen auf unterschiedlichen Ebenen unterstützen. Verfügbare Ressourcen sowie gesellschaftliche Effekte und Nebeneffekte beeinflussen die Entscheidungsfindung, während epidemiologische Parameter eine wichtige Rolle für grundsätzliche Maßnahmensetzungen spielen. Der evidenzbasierte Ansatz des Projekts beruht auf den lessons-learnt der Covid-19-Pandemie sowie den Erfahrungen der AGES und der Projektpartnerorganisationen im Management von epidemischen Entwicklungen bei Mensch, Tier und Pflanze. Das Wissen von Stakeholdern im Public-Health-Bereich wird ebenfalls ergänzend zu einer umfassenden Analyse von Literatur und Dokumenten zum Thema einbezogen. Im Modell werden gesetzliche Handlungsrahmen sowie politische, ethische, sozio-ökonomische und psychologische Aspekte als Werte und Interessen innerhalb der Gesellschaft berücksichtigt. Letztlich trägt (Krisen-)Kommunikation über unterschiedliche Medien und gesellschaftliche Akzeptanz auf verschiedenen Ebenen dazu bei, ob und in welcher Form Entscheidungen im Pandemiemanagement getroffen werden können.

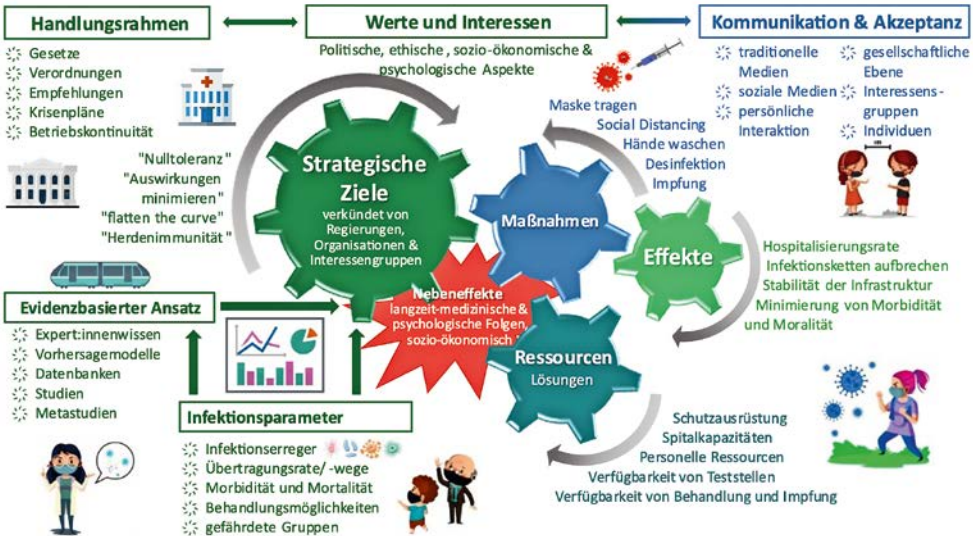


Abb.: Projektübersicht

Projektstand und Aussicht

Nach dem ersten Projektviertel wird im ROADS-Projekt an der Ausarbeitung von Zielsetzungen im Pandemiemanagement geforscht. Die Zielerreichung wird auf strategischer, taktischer und operativer Ebene ausgearbeitet, um Haupt- und Subziele zu identifizieren, die letztendlich durch Maßnahmen und Maßnahmenbündel realisiert wurden. Diese werden weiter herausgearbeitet, zum anderen werden sie auch einer Wirksamkeitsbewertung unterzogen und durch ein Advisory Board aus Expertinnen und Experten auf der Grundlage praktischer Erfahrungen zusammengeführt.

Die Zielsetzungen, die sukzessive auf ihren Ebenen heruntergebrochen wurden:

- Auf strategischer Ebene wurden die Zielsetzungen sehr breit beschrieben, da sie in dieser Form nicht öffentlich kommuniziert werden. Die in Österreich angewandten Strategien (z. B. Durchimpfungsstrategie) wurden durch Beispiele, wie sie international zur Anwendung gekommen sind (z. B. Durchseuchungsstrategie), exemplarisch ergänzt.
- Auf taktischer Ebene wurden drei Zielsetzungen identifiziert: Containment (Eindämmung) – Protection (Schutz von Risikogruppen) – Mitigation (Folgenminderung). Diese werden klassisch in der Epidemie-/Pandemiebewältigung angewandt und überschneiden sich an vielen Stellen.
- Auf operativer Ebene wurden die Zielsetzungen schon fast auf deren Maßnahmen heruntergebrochen und je nach Inhalt Containment, Protection und/oder Mitigation zugeordnet. Für bessere Übersicht und Struktur wurden die operativen Zielsetzungen noch in die Kategorien Datengrundlage, Reduktion der Ausbreitung, Kommunikation, pharmakologische Ziele, Gesundheitsversorgung, Kontakteinschränkung und Auswirkungen abmildern eingeteilt.

Projektleitung:

Österreichische Agentur für Gesundheit

Projektpartner:

- AIT Austrian Institute of Technology GmbH
- Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz
- Gesundheit Österreich GmbH
- Johanniter Österreich Ausbildung und Forschung GmbH
- Medizinische Universität Wien Pentamap GmbH

Kontakt:

DI Mag. DDr. Alois Leidwein
Österreichische Agentur für Gesundheit
Spargelfeldstraße 191
1220 Wien
Tel: +43 664 966 8370
E-Mail: alois.leidwein@ages.at
www.ages.at

ROBOMOLE

ROBOtik für 3D-Mapping, Orientierung und Lokalisierung bei untertägigen Einsatzszenarien

Österreich verfügt aufgrund seiner topografischen Bedingungen über eine Vielzahl an Untertage-Infrastrukturen wie Straßen- und Eisenbahntunnel, U-Bahnen und Stationsbauwerke, Tiefgaragen, Untertage-Bergbauanlagen, Wasserkraftwerke und sonstige Energieversorgungsanlagen sowie Wasserver- und -entsorgungsanlagen. Untertage-Infrastrukturen stellen besondere Herausforderungen für Einsatzkräfte dar. Diese sind neben der außergewöhnlichen körperlichen Anstrengung auch durch spezielle Anforderungen an die Ausrüstung und Einsatztaktik gegeben.

Das Projekt ROBO-MOLE wurde durchgeführt, um bei Einsätzen in Tunnels und sonstigen untertägigen Bauwerken erhöhte Sicherheit für Einsatzkräfte und betroffene Zivilpersonen durch Detektion und Identifikation von Gefahrenstoffen zu gewährleisten, automatisiert Lagekarten zu erstellen sowie einen effizienten Einsatzablauf zu ermöglichen. Beispielsweise stellt ein Gefahrenguttransport-Unfall in einem Tunnel die Einsatzorganisationen aufgrund von Hitze, strukturellen Gefahren, Rauch oder freigesetzten Gefahrenstoffen vor große Herausforderungen. Darum wurde ein semiautonomer Roboter für unterstützende Analyseaufgaben entwickelt, welcher mit positionsgebenden, bildgebenden und gefahrenstofferkennenden Sensoren ausgestattet ist. Diese Sensoren wurden kombiniert, um eine sichere Navigation und Steuerung des Roboters unter schwierigen Untertage-Bedingungen zu ermöglichen und um Gefahren detektieren und kartieren zu können. Dazu arbeiteten im Projekt ROBO-MOLE zahlreiche Projektpartner.

Im Projekt ROBO-MOLE wurden typische Untertage-Szenarien ausgearbeitet und in Anforderungen an die einzusetzende Sensorik übersetzt. Dabei wurde zwischen Sensorik für die Bestimmung der Positions- und Navigationslösung, Sensorik für die Erstellung der 3-D-Umgebungskarten und Schadstoffsensorik unterschieden. Im Rahmen der On-Board-Lokalisierung und Kartenerstellung wurde die Position der mobilen Einheit genau und zuverlässig bestimmt sowie eine moderat aufgelöste Umgebungskarte erstellt. Die Position der mobilen Einheit wurde mithilfe von inertialer Navigation, Radiometrie und LiDAR-Odometrie bestimmt. Diese Daten wurden in Echtzeit mit einem Extended-Kalman-Filter fusioniert. Ferner ist es gelungen in kurzer Zeit adäquate 3-D-Umgebungskarten und informative Lageinformationen zu erstellen. Mit jedem weiteren Scan erweiterte sich das 3-D-Modell. Eine besondere Herausforderung war es, im Tunnel auftretenden Rauch, der sowohl die Sicht als auch die automatische Auswertung beeinträchtigte, effizient zu entfernen. Hierzu wurden geeignete Filter entwickelt. Eine weitere Entwicklung umfasste das Steuerungskonzept für den Roboter im Tunnelszenario, das sowohl direkte Steuerung durch den Operator als auch automatische Wegpunkt-Navigation erlaubt. Zusätzlich wurde eine Onboard-Intelligenz implementiert, die es dem Roboter erlaubt, Aufgaben in verschiedenen Betriebsmodi (teleoperiert, Stop&Go Exploration) zu erledigen. Navigation und Onboard-Steuerung wurden in Integrationstest an der TU Graz und Erprobungen am ZAB evaluiert.

Zum einen wurden dazu Tests der einzelnen Sensorpartner mit dem Roboter durchgeführt, zum anderen wurden Versuche im 1:1-Maßstab in der Untertageanlage am Zentrum am Berg (ZaB) absolviert. Die an der TU Graz und am ZaB durchgeführten Integrationstests hatten zum Ziel, das Zusammenwirken der individuellen Module im Verbund des Gesamtsystems zu testen. Hierzu wurden Tests mit dem Roboter sowie Kalt- und Heißrauch-Versuche mit den Sensorpartnern und den Bedarfsträgern durchgeführt. Ferner wurden die entsprechenden Softwareschnittstellen zu den Onboard-Komponenten am Roboter sowie den Auswerte- und Visualisierungskomponenten im Leitstand implementiert.

Als Testumgebung für die Szenarientests wurde das ZaB in Eisenerz ausgewählt. Es besteht aus zwei parallel geführten Straßen- und zwei parallel geführten Eisenbahntunneln von je 400 Metern Länge, die miteinander untertägig verbunden sind. Die Straßentunnel sind voll ausgebaut und am neuesten Stand der Technik, wodurch eine einzigartige Testumgebung geboten wurde. Für die Validierung am ZaB wurden zwei Testszenarien festgelegt. Im Szenario 1 wurde ein brennendes Auto angenommen, wofür der Straßentunnel mit Kaltrauch vernebelt wurde. Es bestand die Annahme, dass ein brennendes Auto für diesen Rauch verantwortlich ist. Ferner wurde ein Transporter mit gefährlichen Stoffen angenommen. Der Roboter sollte hier die Feuerwehr beim Suchen von verletzten Personen unterstützen. Im Szenario 2 wurde ein Gasaustritt angenommen. Für dieses Szenario wurde eine CO_2-Gasflasche gewählt, die einen Gasaustritt simulieren sollte. Der Roboter, welcher mit einem entsprechenden Gasdetektor ausgestattet wurde, unterstützte auch hier die Feuerwehr.

Durch die Entwicklungen im Projekt ROBO-MOLE werden Einsatzkräfte in Echtzeit mit aktuellen Informationen aus vor Ort aufgenommenen Messwerten direkt beim Einsatz versorgt. Georeferenzierte Messungen zu freigesetzten Gefahrenstoffen und Daten aus 3-D-Scannern werden zur Erfassung der räumlichen Situation semantisch aufbereitet und automatisch in einer Lagekarte übersichtlich dargestellt. Durch den Einsatz eines semiautonomen Roboters, der sich mittels einer Vielzahl von Sensoren selbstständig in der Umgebung lokalisiert und bewegt, können Daten gesammelt werden, ohne dass sich Einsatzkräfte einer zusätzlichen Gefährdung aussetzen. Dadurch trägt ROBO-MOLE wesentlich zum Schutz und zur Verbesserung der Bewältigung gefährlicher Notfalleinsätze bei.

Abb.: Roboter beim Abschlusstest im Straßentunnel am ZaB mit Sichtbehinderung durch Kaltrauch

Projektleitung:

Montanuniversität Leoben – Subsurface Engineering

Projektpartner:

- Zentrum am Berg (ZaB) der Montanuniversität Leoben
- Disaster Competence Network Austria
- Institut für Geodäsie und Institut für Softwaretechnologie der Technischen Universität Graz
- AIT Austrian Institute of Technology – Digital Safety and Security
- JOANNEUM RESEARCH Forschungsgesellschaft mbH – Digital
- Riegl Research Forschungsgesellschaft mbH
- IQSoft GmbH
- CBRN Protection GmbH
- E-NETIC
- Bundesministerium für Landesverteidigung
- Berufsfeuerwehren Graz, Linz und Innsbruck

Kontakt:

Univ.-Prof. Robert Galler
Montanuniversität Leoben
Erzherzog Johann Straße 3
8700 Leoben
Tel: +43 3842 402 3401
E-Mail: Robert.galler@unileoben.ac.at
www.zab.at

SCALA

Sicherheit im urbanen Raum

Motivation und Problemstellung

Die Erfassung, Verfolgung und Bekämpfung von Drohnen ist eine wichtige Aufgabe der öffentlichen Sicherheit. Das Projekt SCALA verfolgt die Erfassung und Verfolgung von Drohnen in urbanen Gebieten sowie deren Bekämpfung durch einen weiträumig verteilten Verbund von multimodalen Sensoren und Aktoren.

Die rasante Entwicklung von unbemannten Kleinst- und Kleinflugsystemen treibt das exponentielle Wachstum der kommerziellen Branche an und stellt eine asymmetrische Bedrohungslage als potenzielles Angriffsmittel vor dem Hintergrund ineffizienter Abwehrmöglichkeiten dar. Allein aus aktueller Technologieprognose ist bereits ersichtlich, dass Flugsysteme im nächsten Evolutionsschritt noch mehr Funktionalität vor allem hinsichtlich deren Autonomie aufweisen werden. Vor dem Hintergrund der zunehmenden Veränderung der sicherheitspolitischen Bedrohungslage ist eine Adaptierung der Bedrohungsszenarien durch Berücksichtigung unbemannter Flugsysteme als potenzielles Angriffsmittel von entscheidender Bedeutung.

Ziele

In diesem Zusammenhang sind die Erfassung, Verfolgung und Bekämpfung von Drohnen eine wichtige Aufgabe der öffentlichen Sicherheit. Vor allem in urbanen Gebieten mit ihren beeindruckenden Skylines behindern hohe Gebäude die Sichtlinie des Beobachters zur Drohne und erschweren deren Erfassung, wodurch bestehende Konzepte an die Grenzen ihrer Möglichkeiten stoßen.

Die übergeordneten Ziele von SCALA sind:

- die Erforschung und Entwicklung einer optimierten Technologie zur Bekämpfung der Bedrohungslage durch Drohnen in städtischen Gebieten durch den Einsatz eines großräumig verteilten multimodalen Sensornetzwerks unter Einbeziehung bestehender verfügbarer städtischer Infrastruktur,
- eine Bewertung der erforschten Technologie anhand behördlich relevanter urbaner Szenarien und
- Empfehlungen für die Regulative.

Abb.: Die vorliegende Abbildung veranschaulicht das Panorama von Wien und verdeutlicht die vielschichtige Struktur einer Metropole, bestehend aus erheblichen Gebäudestrukturen, Verkehrsstraßen und Wegen. Im Kontext dieser städtischen Umgebung ist die SCALA-Technologie nahtlos in die Infrastruktur integriert und bietet ein Instrument zur Bekämpfung der Bedrohungslage durch Drohnen

Die SCALA-Technologie wurde gemeinsam mit den Bedarfsträgern erprobt, um ihre Einsatztauglichkeit anhand der spezifischen Einsatzszenarien und -anforderungen in einem städtischen Umfeld zu evaluieren. Dabei wurden die dezentralen, multimodalen Sensornetzwerke in die bestehende Infrastruktur integriert. Die gewonnenen Erkenntnisse flossen in die Weiterentwicklung der Technologie ein und dienten als Grundlage für die Entwicklung von Regulierungsempfehlungen. Damit leistete SCALA einen wissenschaftlich fundierten Beitrag zur Erhöhung der Sicherheit in urbanen Räumen im Kontext der Drohnenbedrohung.

Projektleitung:

AIT Austrian Institute of Technology GmbH

Projektpartner:

- A1 Telekom Austria AG
- Austria Institut für Europa- und Sicherheitspolitik GmbH
- INRAS GmbH
- Joanneum Research Forschungsgesellschaft mbH
- Bundesministerium für Landesverteidigung
- Bundesministerium für Inneres
- Bundesministerium für Justiz
- Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Kontakt:

DI Christoph Sulzbachner, MSc
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4177
E-Mail: christoph.sulzbachner@ait.ac.at
www.ait.ac.at

SECU

Sicherheitsgefühl der Menschen in neuen Medienlandschaften

Die gesellschaftliche Auseinandersetzung mit Zuwanderung und Terrorismus sowie mit der pandemischen Notlage und zuletzt dem Russisch-Ukrainischen Krieg haben das subjektive Sicherheitsempfinden innerhalb der österreichischen Bevölkerung in den vergangenen Jahren geprägt. Der im Vorfeld der Covid-19-Pandemie verzeichnete Trend hin zu einem stärkeren Gefühl von Sicherheit hat sich dabei umgekehrt: Zuwanderungssorgen, soziale und wirtschaftliche Ängste sowie Besorgnis über Gewaltkriminalität im öffentlichen Raum sind präsenter geworden. Massen- und Individualmedien spielen seit jeher als Informationsquellen und Orte der gesellschaftlichen Diskussion eine zentrale Rolle für das subjektive Sicherheitsempfinden. Soziale Medien und die Verbreitung von Smartphones haben jedoch die Verbreitung, Rezeption und Diskussion sicherheitsrelevanter Information grundlegend verändert und damit bewährte Praktiken einer effizienten und kurz- wie langfristig effektiven Sicherheitskommunikation in Frage gestellt.

Das Projekt Sicherheitsgefühl der Menschen in neuen Medienlandschaften (SECU) erhebt detaillierte Daten zur Rezeption sicherheitsrelevanter Themen in Anbetracht individualisierter Mediengewohnheiten, welche ganzheitlich auf ihren zeitlichen Zusammenhang mit dem individuellen Sicherheitsempfinden in Österreich bewertet werden. Abschließend überprüft es den kausalen Einfluss sozialer Medien und deren Meinungsführer auf das Sicherheitsempfinden und stellt fest, wie öffentliche Sicherheitskommunikation innerhalb der verfügbaren Social-Media-Kanäle aussehen sollte.

Hintergrund

Durch soziale Medien werden für die öffentliche Sicherheit relevante Ereignisse (wie z. B. Terroranschläge oder besondere Fälle von Gewaltkriminalität) blitzschnell verbreitet. Dies kann insgesamt zu dem Eindruck führen, dass Bedrohungen überall und permanent präsent sind. Darüber hinaus lassen es insbesondere Smartphones zu, dass Rezipienten permanent und beiläufig mit personalisierten, sicherheitsrelevanten Informationen konfrontiert werden und soziale Kontakte jedweder Art, d. h. Freunde und Bekannte sowie Fremde, zu deren Diskussion verfügbar sind. Es haben sich auch nicht institutionalisierte Medienangebote etabliert, die sich nicht notwendigerweise den Konventionen guter journalistischer Praxis verpflichtet fühlen und mitunter Falsch- und Fehlinformation verbreiten.

Diese veränderten Medienbedingungen sind hochrelevant für das individuelle Sicherheitsempfinden der österreichischen Bevölkerung, da traditionelle Medienkanäle hierzulande zunehmend an Bedeutung verlieren. Nachrichten werden von immer mehr Menschen vorwiegend mobil auf deren Smartphone rezipiert. Die aktuelle Forschung berücksichtigt die veränderten Medienbedingungen bisher jedoch nur begrenzt, sodass der Einfluss von Smartphones und sozialen Medien bisher nur wenig erforscht ist. Innerhalb der

Sicherheitsforschung gilt die Kultivierungshypothese als etabliert, d.h. die Annahme, dass sich die Berichterstattung zu sicherheitsrelevanten Themen verzerrend auf das subjektive Sicherheitsgefühl der Rezipientinnen und Rezipienten auswirkt. Das vorliegende Projekt beschreitet hierbei innovative Wege, die einen empirischen und praktischen Mehrwert bieten sollen.

Projektziele und methodische Umsetzung

Das vorliegende KIRAS-Projekt verfolgt drei zentrale Projektziele, zu deren Erreichung unterschiedliche methodische Zugänge variabel kombiniert werden. Die einzelnen Zielstellungen adressieren verschiedene Schwerpunkte, die gemeinsam einen ganzheitlichen Ansatz zur Verbesserung der öffentlichen Sicherheitskommunikation in Österreich versprechen.

Ein Scoping Review liefert ein empirisches Fundament und bietet einen Überblick über die seit 2007 publizierte internationale Forschungsliteratur zur Mediennutzung und dem subjektiven Sicherheitsempfinden im öffentlichen Raum. Das Scoping Review erhebt dabei auch die zentralen Forschungslinien und wichtigsten Ergebnisse zum Themengebiet des Projekts. Überdies werden mithilfe von sechs Fokusgruppen mit 31 Menschen aus ganz Österreich die individuellen Mediennutzungsgewohnheiten bei sicherheitsrelevanten Themen in all ihrer Heterogenität untersucht. Die Fokusgruppendiskussionen zeigen zudem, welche Spezifika sozialer Medien (wie z. B. ihre Schnelligkeit, ihr Netzwerkcharakter oder ihre Visualität) im Hinblick auf sicherheitsrelevante Themen als besonders wichtig wahrgenommen und welche Rollen traditionellen und sozialen Medien, separat und in Interaktion, zugewiesen werden.

Aufbauend auf den Ergebnissen der Fokusgruppendiskussionen überprüft eine zweiwellige Panelstudie gezielt den zeitlichen Zusammenhang zwischen individuellen Mediennutzungsgewohnheiten und subjektivem Sicherheitsempfinden. Die Ergebnisse der Panelstudie zeigen nicht nur die jeweiligen Effekte traditioneller und sozialer Mediennutzung, sondern auch deren Interaktion, wodurch erstmalig eine realistische Einschätzung der medienübergreifenden Nutzungsgewohnheiten in Österreich ermöglicht wird. Zudem lässt das Paneldesign eine prädiktive Einschätzung des Einflusses der Mediennutzung auf das subjektive Sicherheitsgefühl der Bevölkerung zu und stellt fest, welche Gewohnheiten für welche Personen bei welchen Inhalten welche Wirkung auf das individuelle Sicherheitsempfinden haben.

Drei Experimente überprüfen abschließend den kausalen Einfluss unterschiedlicher Social-Media-Kommunikatoren und zeigen auf, welche Kommunikationsweisen in unterschiedlichen Situationen strategisch eingesetzt werden können, um aufkommende Empfindungen von Unsicherheit, verursacht durch soziale Medien, in der Bevölkerung durch eine optimierte Sicherheitskommunikation zu begegnen. Ein experimenteller Zugang bietet hierbei die Grundlage für die Untersuchung des kausalen Einflusses spezieller Charakteristika sozialer Medien (wie z. B. die Kommentarfunktion).

Projektleitung:

Universität Wien

Projektpartner:

- Bundesministerium für Inneres

Kontakt:

Univ.-Prof. Dr. Jörg Matthes / Dr. Kevin Koban, M.A.
Institut für Publizistik- und Kommunikationswissenschaft, Universität Wien
Währinger Straße 29
1090 Wien
Tel: +43 1 4277 49307
E-Mail: joerg.matthes@univie.ac.at / kevin.koban@univie.ac.at
www.advertisingresearch.univie.ac.at/

SEWAT

Mikrobiologische und chemo-physikalische Echtzeitparameter zur Qualitätskontrolle in der mobilen Trinkwasseraufbereitung

Für die sichere Nutzung der essenziellen Ressource Trinkwasser ist die Einhaltung mikrobiologischer und chemischer Qualitätskriterien zwingend erforderlich. Die Bereitstellung von sicherem Trinkwasser ist besonders in Krisen- und Katastrophensituationen eine große Herausforderung. Militärische wie auch zivile Organisationen sind bereit, im Falle des Ausfalls oder Mangels an regulärer Trinkwasserinfrastruktur mit verlegbaren Trinkwasseraufbereitungsanlagen Abhilfe zu schaffen. Die gesetzlich vorgeschriebenen Methoden zur Überwachung der mikrobiologischen Wasserqualität liefern meist erst einen Tag nach der Probennahme Auskunft über die Nutzbarkeit des produzierten Trinkwassers. Dies ist für die Überwachung und Steuerung der Aufbereitungsprozesse absolut unzureichend und verzögert eine zeitnahe Versorgung. Das Projekt SEWAT (Save and Efficient Water Treatment) setzt sich nun zum Ziel, mehrere potenzielle Methoden für die Nahe-/Echtzeit-Überwachung der mikrobiologischen und physikalisch-chemischen Wasserqualität zu prüfen. Die Methoden sollten (i) Kontaminationen und Prozessmängel zeitnah, zuverlässig und automatisch erkennen können und (ii) unter den schwierigen Einsatzbedingungen im Feld und bei Einsätzen bedienungssicher und wartungsarm funktionieren. Dabei wird ein „From-source-to-tap"-Ansatz gewählt, der die Wasserqualität vom Rohwasser über die Aufbereitungsschritte bis hin zur Abfüllung und Lagerung beobachtet. Zur Anwendung kommen automatisierte Durchflusszytometrie, enzymaktivitätsbasierende Detektion der Bakterienaktivität, spektrometrische Verfahren für den Online-Nachweis chemischer Verunreinigungen sowie molekular-diagnostische Schnelltests für bakterielle Indikatoren und Pathogene. Darüber hinaus soll auch das Potenzial moderner Mikroskopie- und Durchflusszytometrie-Methoden für die schnelle Detektion von Viruspartikeln ausgelotet werden. Parallel zu diesen technischen Entwicklungen soll eine sozialwissenschaftliche Studie untersuchen, welche Faktoren die Akzeptanz von aufbereitetem Trinkwasser in der versorgten Zielgruppen beeinflussen und wie geeignete Maßnahmen diese Akzeptanz erhöhen können.

Hauptbedarfsträger in diesem Projekt ist das ABC-Abwehrzentrum des Österreichischen Bundesheeres (ÖBH). Weitere Bedarfsträger sind das Wehrwissenschaftliche Institut für Schutztechnologien – ABC-Schutz der Deutschen Bundeswehr (WIS) und die Einheiten für Katastrophenhilfe des Österreichischen Roten Kreuzes (ÖRK). Das Konsortium bildet sich aus den genannten Bedarfsträgern, drei Universitäten (Technische Universität Wien, Medizinische Universität Wien, Karl Landsteiner Privatuniversität für Gesundheitswissenschaften), die sich im Rahmen des Interuniversitären Kooperationszentrums Wasser und Gesundheit (ICC Water&Health) schon lange mit der Entwicklung und Anwendung moderner Nahe-/Echtzeit-Nachweisverfahren für die Bestimmung der mikrobiologischen Wasserqualität befassen. Weiters beteiligt sind drei weltweit führende kommerzielle Anbieter von Technologien für die Nahe-/

Echtzeit-Überwachung der Wasserqualität: bNovate, der schweizerische Anbieter von Online-Durchflusszytometern, s::can, ein österreichischer Hersteller von hochauflösenden Spektrometern, und die VWMS GmbH, einer der führenden Anbieter von Messgeräten für die Vor-Ort-Messung von bakteriellen Enzymaktivitäten in Wasser. Die Konsortialmitglieder können demnach auf umfassende Erfahrungen innerhalb der Themengebiete der gegenständlichen Fragestellung zurückblicken.

Die Ergebnisse dieses Projekts sollen Betreibern von mobilen Wasseraufbereitungsanlagen im militärischen und zivilen (Katastrophen-)Einsatz aufzeigen, welche Rolle moderne Nahe-/Echtzeit-Analysenmethoden in der Prozessüberwachung und -steuerung spielen können. Darüber hinaus können die Erkenntnisse aber auch dazu beitragen, die Qualitätssicherung in der kommunalen Wasserversorgung zu unterstützen und damit die kritische Infrastruktur Österreichs resilienter und krisensicherer zu machen.

Abb. 1: Mobile Wasseraufbereitungsanlage des Österreichischen Bundesheeres

Abb. 2: Detailaufnahme Wasseraufbereitungsanlage des Österreichischen Bundesheeres

Projektleitung:

Technische Universität Wien

Projektpartner:

- Bundesministerium für Landesverteidigung – ABC-Abwehrzentrum
- Deutsches Bundesministerium für Verteidigung – Wehrwissenschaftliche Institut für Schutztechnologien – ABC-Schutz
- Österreichisches Rotes Kreuz
- bNovate SA
- Vienna Water Monitoring Solutions GmbH
- s::can GmbH
- Medizinische Universität Wien – Institut für Hygiene und Angewandte Immunologie
- Karl Landsteiner Privatuniversität für Gesundheitswissenschaften

Kontakt:

DI Dr. Georg Reischer
TU Wien, Institut für Verfahrenstechnik, Umwelttechnik und Technische Biowissenschaften, IFA-Tulln
Konrad-Lorenz-Str. 20
3430 Tulln
Tel: +43 1 58801 166 556
E-Mail: georg.reischer@tuwien.ac.at
www.waterandhealth.at

SHIFT

Sichere Simulationstechnologien für cyber-physische Systeme

Bei vielen kritischen Infrastrukturen handelt es sich um cyber-physische Systeme. Der Begriff CPS beschreibt Systeme, bei denen softwaretechnische mit mechanischen oder elektronischen Komponenten verbunden sind, die über eine Dateninfrastruktur miteinander kommunizieren, wie beispielsweise intelligente Stromnetze, industrielle Steuerungsanlagen oder Satellitennavigationssysteme. Diese Verknüpfung von komplexen und vernetzten Komponenten in einer physischen Umgebung erfordert insbesondere durch die Digitalisierung erhöhte Aufmerksamkeit im Bereich der Sicherheit, Verfügbarkeit und Integrität. Wenn es um die Sicherheit von CPS geht, dann spielen viele Faktoren eine Rolle. Neben dem Einsatz geeigneter Schutzmechanismen sind die Erkennung von Angriffen, deren Eindämmung und die Wiederherstellung der betroffenen Systeme Teil der Maßnahmen zum Umgang mit Cyber-Angriffen[1]. Mit einer geeigneten Simulationsumgebung kann die richtige Reaktion auf Angriffe im Rahmen von Vorfallsübungen in einer geschützten Umgebung trainiert werden. Sie ermöglicht außerdem, Cyberangriffe auf CPS besser zu verstehen, geeignete Gegenmaßnahmen vorzubereiten, neue Algorithmen zur Erkennung von Angriffen zu entwickeln und neue resilientere Architekturen für CPS zu entwerfen. Die Herausforderung bei der Umsetzung ist jedoch, dass viele Technologien für CPS kommerziell lizenziert werden und nur wenige quelloffene Lösungen zur Verfügung stehen. Dies und weitere Faktoren erschweren die Entwicklung von technischen Simulationsumgebungen und verhindern dadurch, dass ein gemeinsames Wissen im Aufbau und der Umsetzung von technischen Simulationsumgebungen für CPS erzeugt werden kann.

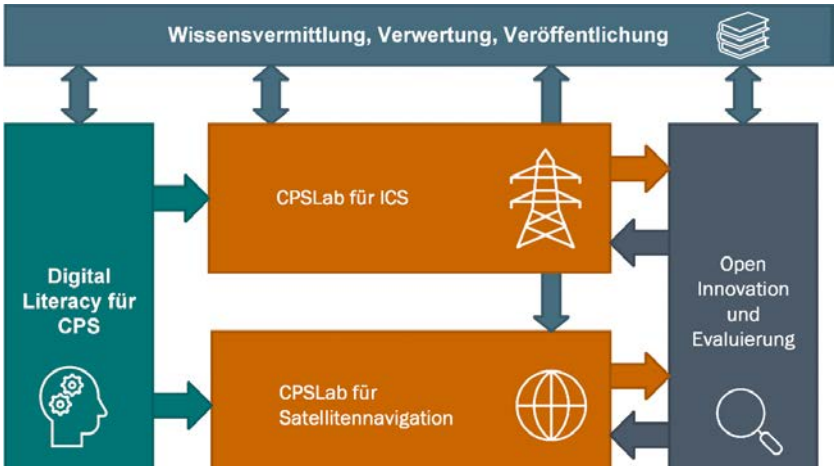


Abb.: Ansatz von SHIFT

1 Barrett, M.: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, https://doi.org/10.6028/NIST.CSWP.04162018,)

Das Projekt SHIFT zielt darauf ab, sichere technische Simulationsumgebungen für CPS zu entwerfen und zu entwickeln. Im Mittelpunkt stehen vier Hauptaspekte:

1. Die Konzeption und Entwicklung von technischen Simulationsumgebungen für CPS für die zwei Anwendungsbereiche industrielle Steuerungsanlagen (ICS) und globale Navigationssatellitensysteme (GNSS) in CPSLabs, einer Laborumgebung für CPS.
2. Die technische Simulation von Cyberangriffen auf ICS und GNSS, die ermöglicht, Konsequenzen von Angriffen zu untersuchen und Algorithmen zur Erkennung zu entwickeln.
3. Förderung und Entwicklung von digitalen Kompetenzen im Bereich CPS für verschiedene Zielgruppen (z. B. Behörden, Betreiber wesentlicher Dienste – BwD) durch z. B. Schulungen oder die Integration in Ausbildungsschienen.
4. Die Einbindung der Benutzerinnen und Benutzer in die Gestaltung und Evaluierung der CPSLabs anhand von Vorfallsübungen oder Schulungen, um eine möglichst hohe Akzeptanz zu erzielen.

Die Nutzung von Cyber Ranges (virtuellen Simulationsumgebungen) ermöglicht, durch eigene Erfahrungen zu lernen. Mit dem CPSLab für industrielle Steuerungsanlagen soll es ermöglicht werden, verschiedene Arten von Cyberangriffen auf industrielle Kontroll- und Steuerungssysteme zu simulieren. Die simulierten Bedrohungen orientieren sich an den Top-10-Bedrohungen für ICS[2], die in unregelmäßigen Abständen vom Deutschen Bundesamt für Sicherheit in der Informationstechnik veröffentlicht werden. Die Simulationsumgebung von SHIFT wird auf eine Anwendung aus dem Energiebereich fokussieren. Der Ansatz berücksichtigt Systeme der IT (Information Technology) und der OT (Operational Technology) gleichermaßen. Letztere bestehen sowohl aus Supervisory-Control- and Data-Acquisition (SCADA)-Systemen als auch aus den Geräten im Feld wie Steuerungen und Sensoren. Das gewählte Konzept ermöglicht es, sowohl die Beschäftigten im Security Operations Centre (SOC) einzubeziehen als auch diejenigen, die eine OT-Umgebung betreiben und warten (d. h. Betriebs- und Wartungspersonal).

Das CPSLab für Satellitennavigation stellt eine Simulationsumgebung für eine wissenschaftliche Untersuchung dar, mit der auch potenzielle Cyberangriffe auf derartige Systeme simuliert werden können. Ziel ist es, die Robustheit und Auswirkungen von Angriffen auf verschiedene Anwendungen zu untersuchen, die auf die Lokalisierung oder das Zeitsignal angewiesen sind, welche von Satellitennavigationssystemen zur Verfügung gestellt werden.

Ein weiteres Ziel von SHIFT ist es, Methoden und Lernmodule zu entwickeln. Dazu werden zunächst Trainingsanforderungen und -bedürfnisse der Stakeholder in Bezug auf Cyber-Security und kritische Infrastrukturen identifiziert, um dann gezielt entsprechende Lernmodule zu erstellen.

Die erarbeiteten Übungen werden schließlich gemeinsam mit verschiedenen Zielgruppen getestet und evaluiert, um das Feedback wieder in die Weiterentwicklung der CPSLabs fließen zu lassen.

Mit den in SHIFT entwickelten Lösungen wird es möglich sein, den richtigen Umgang mit Angriffen realitätsnah zu trainieren, um das Sicherheitsniveau cyber-physischer Systeme anzuheben.

2 Bundesamt für Sicherheit in der Informationstechnik: „Industrial Control System Security: Top-10-Bedrohungen und Gegenmaßnahmen v1.50, 3. Mai 2022

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Austrian Energy CERT
- Bundesministerium für Landesverteidigung
- IGASPIN GmbH
- VERBUND AG
- LINZ NETZ GmbH
- Universität Wien
- Universität für Weiterbildung Krems

Kontakt:

DI Dr. Oliver Jung
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4284
E-Mail: Oliver.Jung@ait.ac.at
www.ait.ac.at/

SiKu KRITIS

Sicherheitskultur in der Kritischen Infrastruktur

Das Projekt beschäftigt sich mit der Konzeptualisierung und Erhebung der „Security Culture“ am Beispiel von drei ausgewählten Organisationen der KRITIS in Österreich

Die kritische Infrastruktur (KRITIS) stellt einen besonders sensiblen Bereich des österreichischen Staates. SiKu KRITIS läuft in einer wichtigen Phase der Neuregulierung und Neuorientierung: Digitale und hybride Angriffe und der Krieg in Europa bringen direkte und indirekte Herausforderungen für die KRITIS-Unternehmen und -Organisationen. Neue Regeln wie die NIS2-Richtlinie und die CER-Richtlinie führen zu einer Ausweitung des Kreises der Betroffenen.

Als ein zentraler Faktor für den Schutz der KRITIS gilt die Sicherheitskultur in Organisationen. Sicherheitskultur in Organisationen wurde bisher hauptsächlich in Zusammenhang mit Unfällen erforscht. Aber, wie die aktuellen Krisen zeigen, vor allem intentionale Gefahren wie Wirtschafts- und Industriespionage, Korruption, Veruntreuung, Cyberangriffe, Diebstähle und Übergriffe auf Mitarbeiterinnen und Mitarbeiter sind zunehmende Bedrohungen für Organisationen der KRITIS. Einige wenige Ansätze zur Messung des Begriffs Security Culture wurden in den vergangenen zehn Jahren entwickelt. Bisher gibt es aber keinen Ansatz, der eine breite wissenschaftliche Konzeptualisierung von Security Culture bietet, ausreichend als Basis für empirische Forschung geeignet wäre und relevante kriminologische Perspektiven, wie die Situational Action Theory von Wikström (2015) sowie die Neutralisationstechnikenthese von Sykes und Matza (1957), zur Erklärung von normwidrigem Verhalten von Mitarbeiterinnen und Mitarbeitern inkludiert. Security Culture kann dadurch bis dato nicht wissenschaftlich erfasst und gestaltet werden.

Der theoretische Fokus liegt daher auf einer umfassenden empirisch relevanten Konzeptualisierung von Security Culture. Diese theoretische Konzeptualisierung wird durch Sicherheitsverantwortliche im Hinblick auf ihre praktische Relevanz validiert (AP2).

Dieses Arbeitspaket befindet sich aktuell (Sommer 2023) in der Abschlussphase. Unter anderem wurde hier mit Fokusgruppen und explorativen Interviews gearbeitet. Mögliche Aspekte von Security Culture finden sich in folgenden Bereichen:

- Bauliche, mechanische und elektronische Gegebenheiten,
- Mitarbeiterinnen und Mitarbeiter/menschliche Aspekte,
- Management,
- Organisation,

- Prozesse sowie
- weitere externe Faktoren.

Aufgrund der hohen Vertraulichkeit im Projekt durch die Beteiligung wesentlicher kritischer Infrastruktur-Unternehmen werden die Dokumentationen nicht veröffentlicht; die Partner erhalten ihre Berichte jeweils einzeln übermittelt. Aus Leitbegriffen wurde weiters eine Visualisierung zu Security Culture generiert, die ein gemeinsames Verständnis fördern soll.

Im empirischen Teil ab Herbst 2023 wird die Sicherheitskultur in Organisationen der KRITIS mit dem Fokus auf intentionale Gefahren erstmalig erhoben und analysiert. Davon umfasst ist die Erforschung der Compliance der Mitarbeiterinnen und Mitarbeiter bezogen auf innerbetriebliche Sicherheitsnormen und die Erklärung von etwaigen Verstößen.

Jeweils ein Unternehmen aus den durch die Krisen besonders betroffenen KRITIS-Sektoren Gesundheit, Energie und Mobilität soll mittels eines im Projekt entwickelten Mixed-Method-Ansatzes aus qualitativer Analyse von sicherheitsrelevanter Infrastruktur und Dokumenten, qualitativen Befragungen von relevanten Schlüsselpersonen sowie Führungskräften und standardisiertem Fragebogen für Mitarbeiterinnen und Mitarbeiter untersucht werden (AP3). Die Erkenntnisse, die aus den aggregierten Ergebnissen gewonnen werden, dienen dazu, Empfehlungen für die gesamte KRITIS abzuleiten, und fließen in eine Publikation ein, die bei einer Fachkonferenz vorgestellt wird. Die Projektergebnisse werden in diesem Rahmen mit Sicherheitsverantwortlichen und -expertinnen/-experten diskutiert (AP4).

Projektleitung:

FH Campus Wien

Projektpartner:

- Wirtschaftskammer Österreich – Stabstelle Krisenmanagement und Sicherheitsvorsorge
- Johannes Kepler Universität – Zentrum für Kriminologie
- Austrian Power Grid AG – Health, Safety, Security & Environment
- ÖBB-Holding AG – Konzernsicherheit
- Wiener Gesundheitsverbund – Prävention und Sicherheitsmanagement

Kontakt:

FH-Prof.in Mag.a Claudia Körmer
FH Campus Wien, Fachbereich Risiko- und Sicherheitsmanagement
Favoritenstraße 226, Raum B.3.10
1100 Wien
Tel: +43 1 606 68 77 2164
E-Mail: claudia.koermer@fh-campuswien.ac.at
ww.fh-campuswien.ac.at

SINBAD

Sicherheit und Prävention vor organisiertem Internet-Bestellbetrug für Anwender durch Maßnahmen der Digitalen Forensik

Im Rahmen des im Oktober 2022 abgeschlossenen Forschungsprojekts SINBAD (Call 19) stand die Skalierbarkeit der KI-basierten Detektion von Fake-Shops und der hierfür benötigte Aus- und Aufbau an Infrastruktur, Tools, Methoden und Prozessen zum Betrieb eines an Konsumentinnen und Konsumenten gerichteten Services im Mittelpunkt. Das Projekt resultierte in der Inbetriebnahme des Fake-Shop Detectors (FSD). Dieser ist eingebettet in einen Lifecycle, bei dem Künstliche-Intelligenz-Analysen, Konsumentinnen/Konsumenten-Meldungen und Schwerpunkt-Erhebungen zusammenwirken. Der Fake-Shop Detector wird kostenlos als Browser-Plugin zur Verfügung gestellt.

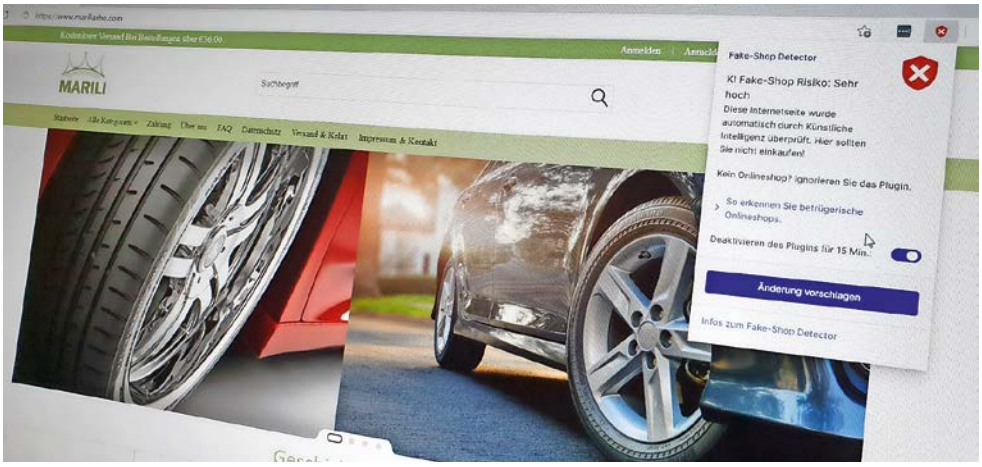


Abb.: Fake-Shops locken Konsumentinnen und Konsumenten mit unglaublichen Angeboten

Das Tool diente im Rahmen des Projekts der wissenschaftlichen Untersuchung der Fragestellungen, inwieweit sich die automatisierte KI-basierte Detektion von Fake-Shops eignet, um (1) den Echtzeit-Schutz von Konsumentinnen und Konsumenten zu garantieren, (2) die Präventionsarbeit technisch unterstützt zu beschleunigen, wie beispielsweise durch ein Screening neu registrierter Domains, (3) und um auch andere Akteure wie Internetservice-Provider im Kampf gegen Cybercrime zu unterstützen.

Der Fake-Shop Detector ist kostenlos über die Browser-Plugin Stores von Firefox, Chrome und Edge verfügbar. Zum Stichtag 31.10.2022 gab es 11.118 bestätigte Blacklist-Einträge sowie 24.530 Whitelist-Einträge in der Middleware des Systems. Die von der KI identifizierten, potenziellen Betrugsfälle werden direkt an die Expertinnen und Experten der Watchlist Internet übermittelt. Die Watchlist Internet ist die

größte deutschsprachige Meldestelle für Internetbetrug, die bislang vor allem basierend auf Meldungen von Konsumentinnen und Konsumenten Warnungen vor Betrugsfallen ausspielte. Der Fake-Shop Detector ist eine disruptive Innovation für die Meldestelle, die seitdem neben Meldungen durch Konsumentinnen und Konsumenten auch KI-Wertungen von Fake-Shops prüft. Sofern die automatisierte Bewertung durch KI einen hohen oder sehr hohen Risikowert ausspielt, prüft das Team der Watchlist Internet manuell das Ergebnis und veröffentlicht in weiterer Folge Domains auf ihrer Warnliste. Der Fake-Shop Detector hat aktuell durchschnittlich 8.000 Userinnen und User täglich und liefert Daten in über 120.000 Requests mit insgesamt über ~22 GB pro Tag aus.

Zum Ende des Projekts lagen der FSD-Middleware bereits 5,36 Millionen Risiko/Ähnlichkeits-Klassifikationen der drei im Einsatz befindlichen KI-Fake-Shop-Modelle (XGBoost, Random Forest, Neural Net) zu insgesamt 1,02 Millionen Domains sowie 2,6 Millionen „Shop/No-Shop"-Klassifikationen der zwei im Einsatz befindlichen KI-Modelle (XGBoost, Random Forest) zu 789.000 Domains vor. Zur Evaluierung der KI-Detektor-Performanz im Echtbetrieb wurde ein Datensatz von 20.391 Web-Shops, die als Blacklist- oder Whitelist-Einträge in der FSD-Middleware geführt werden und somit durch Expertinnen und Experten wie der Watchlist Internet oder FSD-Kooperationspartner manuell gelabeled wurden, herangezogen und mit den Ergebnissen der KI-Einzelmodelle XGBoost, Random Forest, Neural Net sowie des aggregierten Risk-Score-Modells verglichen. Die Treffsicherheit des aggregierten FSD-Gesamtmodells beträgt 88,41% im Praxisbetrieb auf 20.391 Web-Shops, dies ist ein Zuwachs um 1,29% gegenüber der Evaluierung 6/2022. Hierbei zeigt sich auch, dass die Vorschaltung eines eigens trainierten „Shop/No-Shop"-Classifiers Wirkung zeigt.

Zu den weiteren Highlights des Projekts zählen neben diesem Tool für Konsumentinnen und Konsumenten auch eine Studie zur Rolle von Preisen, des Produktangebots und der Kundenansprache von Fake-Shops, eine Studie zu „Crime-as-a-Service"-Angeboten wie z. B. Fake-Shop-Baukastensystemen auf Marktplätzen und Foren des Dark Web und eine Studie zur Akzeptanz, dem Nutzen und dem Potenzial des Echtzeit-Schutzes durch KI, die bestätigt, dass das entwickelte Tool viele Nutzerinnen und Nutzer in der Praxis vor Schaden bewahrt und umfassende Erkenntnisse liefert über ihre Erwartungen an und ihr Vertrauen in KI. Der Fake-Shop Detector wurde in der Praxis übernommen und ist zu einem wichtigen Tool für die Expertinnen und Experten der Watchlist Internet geworden.

Projektleitung:

Österreichisches Institut für angewandte Telekommunikation

Projektpartner:

- AIT Austrian Institute of Technology GmbH
- Ciuvo GmbH
- X-NET Services GmbH
- Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (Bedarfsträger)

Kontakt:

Louise Beltzung
Österreichisches Institut für angewandte Telekommunikation (ÖIAT)
Ungargasse 64–66/3/404
1030 Wien
Tel: +43 1 595 2112
E-Mail: beltzung@oiat.at
www.malzwei.at

SkillDrill

Mixed Reality Trainingsframework für das Trainieren von grundlegenden Skills im Einsatzwesen und von zivilen Experten für den Einsatz bei Krisensituationen

Die gemeinsame Sicherheits- und Verteidigungspolitik (GSVP) der EU soll das zivile und militärische Krisenmanagement stärken. Um die vielschichtigen Herausforderungen hinsichtlich Friedenssicherung, Konfliktverhütung und Stärkung der internationalen Sicherheit effizient zu bewältigen, bedarf es u. a. entsprechend qualifizierten Personals. Aus diesem Grund wurden von der Europäischen Union Ausbildungsinstitutionen und Trainingsinitiativen geschaffen, die sowohl allgemeine Missionsvorbereitung als auch kontext- und mandatsspezifische Themen umfassen.

Ausbildungsinhalte reichen von den richtigen vorbereitenden Planungsmaßnahmen einer Mission bis hin zu spezialisierten Kursen wie HEAT-Trainings, in denen die Teilnehmenden auf das richtige Verhalten in hochkritischen Gefährdungssituationen geschult werden.

Im Rahmen des Krisenmanagements (z. B. im internationalen Hilfs- und Katastrophenmanagement) müssen viele Stakeholder zusammenspielen. Dazu zählen zivile, militärische, diplomatische und humanitäre Akteure.

Dazu sind umfangreiche Fähigkeiten der entsandten Personen erforderlich (z. B. Monitoring, Mediation, interkulturelle Kompetenzen, Entscheidungsfindung). Diese werden in entsprechenden Ausbildungen bestehend aus Theorie und praktischen Übungen vermittelt.
Virtual Reality (VR) und Mixed Reality (MR) bieten neue Möglichkeiten, um wirksam und kostengünstig zu trainieren. Im Projekt wird daher ein VR/MR-Trainingsframework erstellt, mit dem grundlegende, von den Bedarfsträgern benötigte Skills mit geringem Aufwand immersiv vermittelt werden können.

Ziel ist, ein Trainingssystem zu erstellen, mit dem auf drei Immersionsebenen essenzielle Skills für Planung und Einsatzvorbereitung von Auslandsmissionen trainiert werden. Dieser Rahmen bildet alle Bereiche von der strategischen Planung bis zur Patientenversorgung ab und erlaubt die Einbeziehung soziokultureller Aspekte.
Die ***digitale*** Ebene bietet Kursinhalte zur strategischen Planung. Die ***VR***-Ebene bietet Kursinhalte zur Einsatzvorbereitung. Grundlegende Skills, die zivile Fachkräfte am Einsatzort benötigen, können mittels VR-Technologie immersiv trainiert werden. Der Fokus liegt auf Safety & Security (z. B. Verhalten an

Checkpoints) sowie Verhandlungs- und interkulturellem Kompetenztraining. Trainings können allein oder gemeinsam – ortsunabhängig – mit anderen Trainierenden durchgeführt werden.
Die ***MR***-Ebene bietet darüber hinaus Inhalte, die dank moderner MR-Technologie noch immersiver trainiert werden können. Hier ist die Versorgung von Verletzten in Krisengebieten zu erwähnen, die durch Einbezug von Übungspuppen und nötiger Notfall-Ausrüstung effizienter trainiert werden kann. Diese Elemente werden in das System implementiert und im vorab definierten VR-Szenario entsprechend dargestellt. So kann die Versorgung an der Puppe im virtuellen und dynamischen Umfeld einer Auslandsmission realitätsnah trainiert werden.

Das Projekt hat das Ziel, realitätsnähe Trainingsszenarien zu konzipieren, damit höchstmögliche Trainingseffizienz nachhaltig sichergestellt werden kann. Dazu werden umfassende Szenarienanalysen mit den verschiedenen Bedarfsträgern in engem Abgleich mit den Möglichkeiten modernster digitaler Technologien durchgeführt. Darüber hinaus verfolgt das Projekt einen nutzerzentrierten Ansatz mit Szenario-Workshops und Zwischenevaluierungsworkshops, um eine bedarfsorientierte Entwicklung zu gewährleisten.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Bundesministerin für Europäische und Internationale Angelegenheiten (BMEIA)
- Bundesministerium für Landesverteidigung (BMLV)
- Austrian Centre for Peace (ACP)
- Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH
- MINDCONSOLE GmbH

Kontakt:

Elisabeth Broneder
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 664 8251374
E-Mail: elisabeth.broneder@ait.ac.at
www.ait.ac.at

SYRI

Systemische Risikoanalyse Lebensmittel-Versorgungssicherheit

Zur Bewältigung von lokal isolierten Versorgungsengpässen oder Knappheiten sind analoge Informationsverarbeitung und -wiedergabe häufig ausreichend. Bei großen Krisen, wie die Covid-19-Pandemie, wurden jedoch die Grenzen des analogen und stets vergangenheitsorientierten Krisenmanagements augenscheinlich. Insbesondere bei der Lebensmittelversorgung der Bevölkerung hat sich gezeigt, dass auf staatlicher Ebene nicht ausreichend Daten und Informationen zum Monitoring vorhanden waren, die in der Folge auch nicht an die Bevölkerung kommuniziert werden konnten. Dies liegt daran, dass Lebensmittellieferketten aus komplexen, dynamischen und voneinander abhängigen Akteursebenen in Wertschöpfungsstufen (von der Urproduktion bis zu Konsumentinnen und Konsumenten) bestehen. Die Fähigkeit zur proaktiven und zeitnahen Einschätzung und Analyse von Krisenszenarien ist jedoch von besonderer Bedeutung, da diese unmittelbar für die Versorgung der Bevölkerung mit Lebensmitteln negativ wirken können. Um diesen Herausforderungen zu begegnen, wird für die beiden Bedarfsträger Bundesministerium für Landwirtschaft, Regionen und Tourismus und AgrarMarkt Austria im Zuge des SYRI-Projektes ein digitales, systemisches Risikomonitoring in der Lebensmittelbranche realisiert, welches vom Bundesministerium für Finanzen gefördert wurde.

Für das Echtzeit-Monitoring wird im Projekt SYRI von der Fachhochschule Oberösterreich (Logistikum Steyr), dem Complexity Science Hub, der Universität für Bodenkultur und der Veterinärmedizinischen Universität Wien erstmals auf nationaler Ebene ein digitaler Krisenmonitor für fünf definierte Produktgruppen aufgebaut. Dieser digitale Krisenmonitor ermöglicht durch die Entwicklung eines generischen Datenmodells die erstmalige digitale Erfassung von Wertschöpfungsnetzwerken durch Verschränkung von Bedarfsträger- und Unternehmensdaten aus der Lebensmittelbranche in Österreich, die daraufhin dynamische Berechnungen systemischer Risikokennzahlen auf Akteursebene zulassen. Neben der Sammlung von quantitativen Daten werden zusätzlich qualitative Daten zur Risikoeinschätzung in der Lebensmittellieferkette auf akteurspezifischer Ebene erhoben, um Vulnerabilitäten von Unternehmen, aber auch der Bevölkerung berücksichtigen zu können. Dieses Gesamtbild soll es zukünftig den Bedarfsträgern ermöglichen, im Krisenfall datengetriebene Entscheidungen zur Sicherstellung der Lebensmittelversorgung zu treffen und diese auch entsprechend zielgruppenorientiert zu kommunizieren.

Zwischenergebnisse

Im bisherigen Projektverlauf wurden die Vulnerabilitäten der Bevölkerung und die Risikofelder der Unternehmen der Wertschöpfungsketten der österreichischen Lebensmittelbranche weitgehend abgebildet. In Bezug auf die österreichische Bevölkerung zeigte sich, dass aus der alltäglichen Praxis heraus Nahrungsmittel bevorratet werden, die nicht zwangsläufig die individuelle Krisenresilienz erhöhen, da

nur wenige Bewusstsein über krisensichere Bevorratungsstrategien haben. Die Erkenntnisse legen nahe, dass dieser Umstand auf ein eingeschränktes Risiko- und Gefahrenbewusstsein zurückzuführen ist, da die Wahrscheinlichkeiten für das Eintreten von Krisen nur schwer eingeschätzt werden können. Die vom SORA Institut durchgeführten Untersuchungen haben darüber hinaus die Vermutung nahegelegt, dass die sogenannten Hamster- oder Panikkäufe in Krisenzeiten vor allem auf unzureichende oder widersprüchliche Informationen zurückzuführen sind. Daher ist neben der tatsächlichen Versorgung der Bevölkerung auch die Kommunikation über die zu ergreifenden Maßnahmen und die aktuelle Lage von entscheidender Bedeutung.

Auch in Bezug auf die Vulnerabilität von Unternehmen der Lebensmittelbranche wurden bereits erste Erkenntnisse gewonnen. Diese zeigen, dass quantitative Angaben (z. B. Bestandsdaten, Bewegungsdaten) zu möglichen Lieferengpässen zur optimalen Reaktion nicht ausreichend sind. Insbesondere die damit verbundenen deskriptiven qualitativen Daten über die Ursache der Störung sind erforderlich, um geeignete und vorausschauende Maßnahmen ergreifen zu können. Ein wichtiger Indikator für geeignete Maßnahmen ist dabei vor allem die voraussichtliche Dauer der Lieferkettenunterbrechung. Andernfalls besteht die Gefahr, dass die Unternehmen einen „Bullwhip-Effekt" auslösen, indem sie die Ereignisse überinterpretieren und die Bestellmengen entsprechend nach oben korrigieren: eine Situation, die im Hinblick auf die zum Teil geringe Haltbarkeit von Lebensmitteln zu Problemen führen kann. Aus diesem Grund ist eine umfassende Erfassung der Risiken im Lebensmittelsektor und damit auch deren Abbildung in einem Monitoring-Tool für erhöhte Transparenz notwendig.

Ausblick

Durch die Bündelung der Expertisen von Fachhochschule Oberösterreich (Logistikum Steyr), Complexity Science Hub, Universität für Bodenkultur und Veterinärmedizinischer Universität Wien wurde das Grundgerüst eines Krisenmonitoringtools im Lebensmittelbereich geschaffen. In den noch laufenden finalen Projektphasen gilt es nun, die Risikolandschaft für Lebensmittelunternehmen zu vervollständigen und das Monitoringtool auf Basis der Bestandsdaten der teilnehmenden Unternehmen zu finalisieren. Damit soll nicht nur den Bedarfsträgern in künftigen Krisenfällen die Früherkennung von Lieferengpässen erleichtert, sondern auch den Unternehmen der Lebensmittelindustrie mehr Transparenz in ihren Versorgungsketten ermöglicht werden.

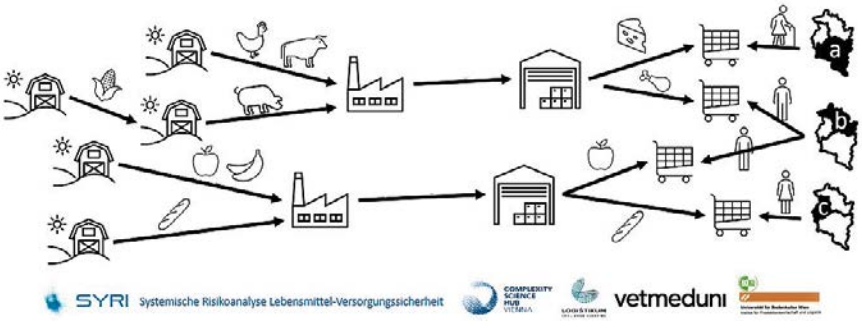


Abb.: Darstellung der Versorgungswege für die Lebensmittel-Versorgungssicherheit

Projektleitung:

FH OÖ Forschungs & Entwicklungs GmbH

Projektpartner:

- Agrarmarkt Austria
- BOKU, Institut fur Produktionswirtschaft und Logisik
- Bundesministerium für Landwirtschaft, Regionen und Tourismus
- Complexity Science Hub Vienna CSH
- Fixkraft-Futtermittel GmbH
- Garant – Tiernahrung Gesellschaft m.b.H.
- Hofer KG
- LGV Sonnengemüse eingetragene Genossenschaft
- REWE International Lager- und Transportgesellschaft m.b.H.
- S. Spitz GmbH
- Top Team Zentraleinkauf GmbH
- Veterinärmedizinische Universität Wien

Kontakt:

Mag. Michael Herburger, BA MA
FH OÖ Forschungs & Entwicklungs GmbH
Wehrgrabengasse 1–3
4400 Steyr
Tel: +43 5 0804 33255
E-mail: michael.herburger@fh-steyr.at
www.forschung.fh-ooe.at

UASwarm

Selbstorganisierende UAS-Schwärme zur Einsatzunterstützung in Katastrophenfällen und bei der Vermisstensuche

Innovative technische Lösungen zur multimodalen Unterstützung des Risiko- und Katastrophenmanagements (zur optimierten Einsatzführung und zum effizienten Ressourceneinsatz) gewinnen immer mehr an Bedeutung. Dadurch soll es auch zur Reduktion der Gefährdung der Einsatzkräfte kommen. Immer öfter auftretende Naturkatastrophen, inkl. der zum Teil damit in Verbindung stehenden Suche nach vermissten Personen, stellen die Einsatzorganisationen sowie die beteiligten Strukturen (BMI, BMLV, Länder, SKKM-Akteure etc.) vor immense Herausforderungen. Lagebeurteilungen und Suchmaßnahmen aus der Luft sind einerseits wesentlich, um z. B. der Feuerwehr, dem Heer, der Rettung etc. die entsprechenden Informationen und Entscheidungsgrundlagen zu liefern. Andererseits können diese eine wesentliche zeitliche Verkürzung der Suchmaßnahmen herbeiführen, was speziell bei Verletzten entscheidend ist. Ziel ist dabei eine Grundlage für Entscheidungen zur Bewältigung der Lage und der größtmögliche Schutz von Menschenleben und kritischer Infrastruktur sowie die Reduktion von Sach- und Umweltauswirkungen, speziell in Waldbrandsituationen (z. B. Glutnestbekämpfung) oder bei der Vermisstensuche.

UASwarm zielt auf den Einsatz von autonomen selbstorganisierenden UAS-Schwärmen (Unmanned Aircraft System, Drohnen) als Monitoring System ab, welches in der Lage ist, in nahezu Echtzeit Informationen aus einem betroffenen Gebiet in o. g. Szenarien zu übermitteln und die Lagebilderstellung, Vermisstensuche als auch die Fortschrittskontrolle von Lösch- und Rettungsarbeiten zu ermöglichen.

Schwärme bringen Zeitvorteile und können größere Gebiete abdecken als einzelne UAS. Der Vorteil selbstorganisierender Schwärme im Vergleich zu mehreren einzelnen zentral gesteuerten UAS (wie z. B. bei Drohnenshows) ist die hohe Adaptivität und Resilienz gegenüber dynamischen Veränderungen in der Umgebung als auch hinsichtlich der Mission selbst. Selbstheilungseigenschaften verkraften den Ausfall einzelner Komponenten, ohne die Mission zu gefährden, und der Betrieb erfordert kaum menschliches Eingreifen. Dies erleichtert die Einbindung in die Prozesse der Einsatzkräfte.
Eine am Anfang des Projektes durchgeführte Szenarien- und Anforderungsanalyse ergab die Zielszenarien Glutnesterkennung in der Nachbearbeitung bei der Waldbrandbekämpfung als auch Vermisstensuche.

Zur Ermöglichung von UAS-Schwärmen in o. g. Szenarien wurden einige technische Kernkomponenten im Projekt entwickelt und getestet. Dazu gehören die

- Schwarmkoordination unterschiedlicher UAS,
- Navigation ohne GNSS-Signal,

- robuste Echtzeit- und Breitbandkommunikation im Schwarm,
- schwarmfähige Flugplattformen,
- leichte, szenarienangepasste Multi-Sensorplattformen (VIS, NIR etc.) und
- KI-basierte echtzeitfähige Fusion sowie Auswertung und Informationsgewinnung (Lagebilderstellung) aus den Daten des Schwarms.

Parallel wurden während des gesamten Projektes sozialwissenschaftliche Aspekte zur Akzeptanz und Verwendbarkeit eines UASwarm-basierten Systems analysiert.

Der Drohnenschwarm-Demonstrator wurde in mehreren Versuchskampagnen getestet und final im Juni 2023 vor Stakeholdern vorgeführt. Er hat in diesen Versuchen gezeigt, dass Glutnester in Waldbrandszenarien verlässlich identifiziert und deren Lage in Form von GPS-Koordinaten sowohl an eine Einsatzleitzentrale als auch auf Smartphone-Apps der Einsatzkräfte übermittelt und in Lagebildkarten dargestellt werden konnten. Auch Personen konnten in ähnlicher Weise erkannt und lokalisiert werden. Aus dem Projekt konnten wichtige Informationen zur weiteren Ausgestaltung des UASwarm-Systems gewonnen werden, insbesondere hinsichtlich der Einbindung in die Prozesse der Einsatzorganisationen.

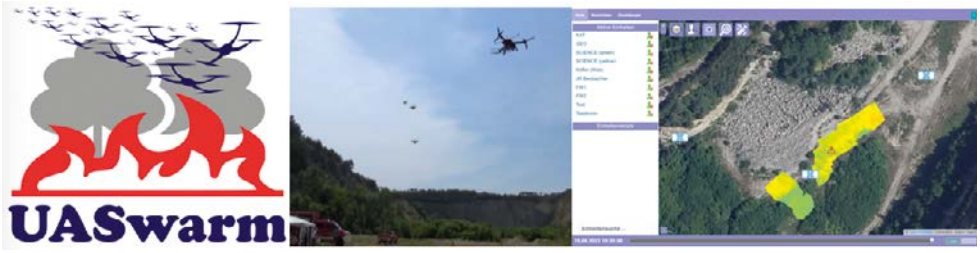


Abb.: Selbstorganisierende UAS-Schwärme helfen in Katastrophenfällen und bei der Vermisstensuche

Projektleitung:

Lakeside Labs GmbH

Projektpartner:

- JOANNEUM RESEARCH Forschungsges.mbH, DIGITAL
- AIT Austrian Institute of Technology GmbH
- Institut f. Intelligente Systemtechnologien, Universität Klagenfurt
- IFR - Ing. Richard Feischl
- Agentur für Europäische Integration und wirtschaftliche Entwicklung GmbH
- LEADER Photonics GmbH
- Freiwillige Feuerwehr Gumpoldskirchen
- Bundesministerium für Landesverteidigung

Kontakt:

Dr. Andreas Kercek
Lakeside Labs GmbH
Lakeside Park B04b
9020 Klagenfurt
AUSTRIA
Tel: +43 463 287 044 33
E-Mail: andreas.kercek@lakeside-labs.com
www.lakeside-labs.com

UAV-Rescue

UAV-getragene Sensorik zur KI-basierten Unterstützung von Rettungsmissionen

In Katastrophenfällen wie etwa Gasexplosionen, Naturereignissen oder auch bei Terroranschlägen kann es zum teilweisen Kollaps von Gebäuden kommen, wodurch die Suche nach Vermissten ein gefährliches und schwieriges Unterfangen wird. Es gilt, die Unglücksopfer möglichst rasch zu retten, da in der „goldenen Stunde" nach dem Ereignis die Überlebenschancen am höchsten sind. Mindestens genauso wichtig ist allerdings auch die Sicherheit der Rettungskräfte: Sie sollen bei den Rettungsmaßnahmen nicht selbst ihr Leben riskieren. Denn nach dem eigentlichen Unglück kommt es häufig zu plötzlichen Einstürzen im Trümmerfeld oder dem Austritt von gefährlichen Gasen aus gerissenen Leitungen.

Die im Projekt UAV-Rescue entwickelten Technologien unterstützen die Einsatzkräfte dabei, schneller und sicherer situationsgerechte Entscheidungen zu treffen. Dazu wurde ein experimentelles Erkundungssystem entwickelt, das auf mehreren (semi-)autonom fliegenden Drohnen (Unmanned Aerial Vehicle – UAV) aufbaut. Das System stellt den Einsatzkräften neben einem taktischen 2-dimensionalen Lagebild eine vollständige 3-dimensionale Lagekarte des Einsatzgebiets in Echtzeit zur Verfügung, ohne dass sie dazu das Trümmerfeld betreten müssen. Die wesentlichen Vorteile bestehen darin, dass das System (i) im Lagebild auch schwer einsehbare Bereiche detailliert kartiert, (ii) Gebäudeschäden bzw. Trümmerhaufen erkennt und analysiert, (iii) Personen lokalisiert sowie (iv) die Einsatzkräfte über mögliche Gefahren wie den Austritt von Gasen informiert.

Das Projekt UAV-Rescue ist eine bilaterale Initiative zwischen Österreich und Deutschland. Die Projektpartner bilden ein hervorragendes Konsortium für die Entwicklung einer UAV-gestützten Lösung für die Unterstützung von Einsatzkräften in Katastrophensituationen.

Der österreichische Teil, geleitet vom AIT Austrian Institute of Technology GmbH, fokussiert sich dabei auf die automatische Analyse des Außenbereichs und die Darstellung des Einsatzraumes in 2- und 3-dimensionalen Lagekarten. Ein weiterer österreichischer Forschungspartner ist die Technische Universität Graz. Die Bedarfsträger und weitere Projektpartner bringen ihre weitreichende Erfahrung mit Großschadenslagen in das Projekt ein: die Berufsfeuerwehren Wien und Linz, die Bundesministerien für Landesverteidigung und für Inneres, die Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH sowie das Disaster Competence Network Austria. Als Industriepartner komplettieren die Unternehmen Rosenbauer International AG, die CBRN Protection GmbH und die Skyability GmbH das Konsortium. Die Projektergebnisse und der Know-how-Gewinn aus dem Projekt werden ihre technologische Wettbewerbsfähigkeit erhöhen und ihnen dadurch ermöglichen, in naher Zukunft neue Geschäftsfelder zu erschließen.

Der deutsche Partnerverbund ergänzt das UAV-Rescue System durch eine (semi-)autonome KI-basierte (künstliche Intelligenz) Erkundung des Innenbereichs sowie die luftgestützte Personendetektion mittels 360°-Radarsensoren.

Abb.: UAV mit Laserscanner

Grundlage der Erkundung im Außenbereich des UAV-Rescue Systems ist die rasche Erfassung eines 3-dimensionalen Abbilds des Katastrophengebiets durch präzise Laservermessung während des Überfliegens mit der Drohne, was typischerweise innerhalb weniger Minuten durchgeführt werden kann. Mittels künstlicher Intelligenz werden in der 3-dimensionalen „Punktwolke", die das Katastrophengebiet repräsentiert, beschädigte Gebäude und Trümmerhaufen in Echtzeit automatisch lokalisiert. Durch 3-dimensionale Umgebungsanalyse werden auch anspruchsvolle semiautomatische UAV-Flugmanöver im Nahbereich von eingestürzten Strukturen ermöglicht, die andernfalls kaum betreten oder durchsucht werden könnten. Laufende Gasmessungen komplettieren die messtechnische Erfassung und werden in die allgemeine Gefahrenabschätzung mit einbezogen. Darüber wird ein Konzept zur automatisierten bautechnischen Risikobewertung, mit der die Resttragfähigkeit von kollabierten Gebäudestrukturen abgeschätzt werden kann, erstellt.
Im Detail beruht die Analyse auf einem neuronalen Netzwerk (KI) zur Segmentierung von 3-dimensionalen Geländedaten. Dabei können auch rasch und für die Einsatzkräfte gefahrlos Bereiche automatisiert analysiert werden, die aufgrund von Verdeckungen durch andere Strukturen anderweitig nicht ohne Weiteres einsehbar wären.
Die Visualisierung aller gesammelten Daten und Messwerte in einer 2-dimenstionalen taktischen Karte zum Einsatzmanagement sowie einer 3-dimensionalen Lagekarte beider Partnerverbünde steht als Benutzerschnittstelle zur Verfügung.

Dank der konsolidierten Darstellung aller aufgenommenen Daten werden die Einsatzkräfte dabei unterstützt, die Rettungsmaßnahmen schneller und sicherer durchzuführen. Bei einer Einsatzübung mit mehreren Einsatzorganisationen wurde das UAV-Rescue System erprobt und evaluiert. Von den Einsatzkräften konnte äußerst positives Feedback zum Mehrwert der durch das System generierten Informationen gesammelt werden.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Bundesministerium für Landesverteidigung
- Bundesministerium für Inneres
- Disaster Competence Network Austria – Kompetenznetzwerk für Katastrophenprävention
- CBRN Protection GmbH
- Johanniter Österreich Ausbildung und Forschung gemeinnützige GmbH
- Berufsfeuerwehr Linz
- Berufsfeuerwehr Wien
- Skyability GesmbH
- Rosenbauer International AG
- Technische Universität Graz – Institut für Tragwerksentwurf

Kontakt:

Dipl.-Ing. Michael Hofstätter
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 50550 4202
E-Mail: michael.hofstaetter@ait.ac.at
www.ait.ac.at

USKIT

Unbemannter Schutz Kritischer Infrastruktur

Motivation und Problemstellung

Die Erfassung, Verfolgung und Bekämpfung von Drohnen ist eine wichtige Aufgabe der öffentlichen Sicherheit. Das Projekt USKIT verfolgt den Einsatz selbstorganisierter Drohnenschwärme zur Luftraumüberwachung sowie Untersuchung von Interventionsmaßnahmen zur Abwehr.

Die rasante Entwicklung von unbemannten Kleinst- und Kleinflugsystemen treibt das exponentielle Wachstum der kommerziellen Branche an und stellt eine asymmetrische Bedrohungslage als potenzielles Angriffsmittel vor dem Hintergrund ineffizienter Abwehrmöglichkeiten dar. Allein aus aktueller Technologieprognose ist bereits ersichtlich, dass Flugsysteme im nächsten Evolutionsschritt noch mehr Funktionalität vor allem hinsichtlich deren Autonomie aufweisen werden. Vor dem Hintergrund der zunehmenden Veränderung der sicherheitspolitischen Bedrohungslage ist eine Adaptierung der Bedrohungsszenarien durch Berücksichtigung unbemannter Flugsysteme als potenzielles Angriffsmittel von entscheidender Bedeutung.

Ziele

In diesem Zusammenhang sind die Erfassung, Verfolgung und Bekämpfung von Drohnen eine wichtige Aufgabe der öffentlichen Sicherheit. Um die Bedrohung gezielt bekämpfen zu können, werden in USKIT selbstorganisierte Drohnenschwärme zur Luftraumüberwachung zusätzlich zur bestehenden verteilten und vernetzten Bodensensorik eingesetzt. Bei den Interventionsmaßnahmen werden kooperative physikalische sowie nachrichtentechnische Maßnahmen untersucht.

Dabei liefert USKIT folgende Ergebnisse:

- Technologie zur kooperativen Luftaufklärung im Schwarmverbund durch einen Starrflüglerschwarm mit multimodaler Sensorik und Vernetzung zur kooperativen Luftraumaufklärung,
- Technologie zur Selbstorganisation eines heterogenen Schwarmverbunds durch Methoden und Verfahren zur selbstorganisierten dezentralen Verwaltung eines skalierbaren heterogenen Drohnenschwarms und
- Technologie zur Intervention im Schwarmverbund mit kooperativen Maßnahmen.

Abb.: Die Abbildung zeigt selbstorganisierte Drohnenschwärme, die zur Überwachung des Luftraums verwendet werden. Diese sind dabei mit fortschrittlicher multimodaler Sensorik und eingebetteten Systemen zur Echtzeit-Datenverarbeitung ausgestattet

USKIT ist ein laufendes Forschungsprojekt und befindet sich derzeit in verschiedenen Entwicklungsphasen. Dazu gehört die Sensorintegration in die Fluggeräte, die Verbesserung der Selbstorganisationsmethoden im Schwarm und die Integration der kooperativen Interventionsmaßnahmen. Im Anschluss sind fortlaufende Tests und Anpassungen notwendig, um die Projektziele zu erreichen. Dies erfordert eine ganzheitliche Herangehensweise, die technische, algorithmische und methodische Aspekte gleichermaßen berücksichtigt.

Projektleitung:

AIT Austrian Institute of Technology

Projektpartner:

- Austria Institut für Europa- und Sicherheitspolitik GmbH
- Joanneum Research Forschungsgesellschaft mbH
- Joby Austria GmbH
- Lakeside Labs GmbH
- Twins GmbH
- Bundesministerium für Landesverteidigung

Kontakt:

D.I.(FH) Christoph Sulzbachner, MSc.
AIT Austrian Institute of Technology GmbH
Giefinggasse 4
1210 Wien
Tel: +43 664 825 1342

WLV.neu

Wirtschaftliche Landesverteidigung NEU

Im ersten Teil des Forschungsprojekts erfolgte eine eingehende Analyse der verfassungsrechtlichen Grundlage für die sog. „umfassende Landesverteidigung“ (ULV). Dabei wurde als Teilaspekt die „wirtschaftliche Landesverteidigung“ (WLV) schwergewichtig ausgeleuchtet. Der Verfassungsgesetzgeber lässt in Art. 9a B-VG einen so weiten Spielraum, dass die Bewältigung aktueller sicherheitspolitischer Risiken mit wirtschaftlicher Relevanz nach wie vor verfassungsrechtlich vom 1975 gesteckten Staatsziel der WLV grundsätzlich gedeckt ist. Eine Anpassung des Art. 9a B-VG scheint in dieser Hinsicht nicht notwendig.

Einfachgesetzlich gestaltet sich die Rechtslage komplexer; insoweit kann eine Zersplitterung der Rechtslage festgestellt werden, die den operativen Vollzug vor große Herausforderungen stellt. Es fehlt der Verwaltung zudem insbesondere die Programmierung zur strategischen Vorausschau, die präventive Maßnahmen der Krisenvorsorge im Sinne der Versorgungssicherheit zur Erzielung systemischer Resilienz überhaupt erst ermöglicht. Schließlich schöpft der Staat durch das primäre Abstellen des Gesetzgebers auf die Wirtschaftslenkung zur Erreichung des Staatsziels WLV von vorneherein sein Potenzial nicht aus.

Diese Zusammenfassung der Herausforderungen auf einfachgesetzlicher Ebene ließ zwei Spannungsfelder zum Verfassungsrecht hervortreten. Einerseits besteht ein Spannungsfeld zum Effizienzgrundsatz staatlichen Handelns und dessen Ausprägung als Effektivitätserfordernis. Es können weiters, ohne die regelmäßige Durchführung einer strategischen Vorausschau (welche Krisenszenarien und, daraus abgeleitet, Vulnerabilitäten evaluiert), die Aufgaben, die der Gesetzgeber regelmäßig in den Lenkungsgesetzen der Verwaltung aufträgt, von dieser nicht effektiv durchgeführt werden, da die Verwaltung jeweils nur auf die Lage reagierend (reaktiv) diese Aufgaben wahrnehmen und dadurch im Endeffekt nie vor die Lage kommen kann. Andererseits betraut der Gesetzgeber die Verwaltung auch mit Aufgaben, ohne die dafür zur Verfügung stehenden Mittel detailliert zu spezifizieren. Aus diesen beiden Überlegungen scheint dogmatisch begründet, dass das Staatsziel WLV es notwendig macht, eine einfachgesetzlich gebündelte Normierung der behördlichen Zuständigkeiten zur Verfolgung dieses Ziels vorzunehmen.

Auf der Grundlage dieser zentralen Erkenntnisse zur aktuellen Verfassungsrechtslage und daraus gewonnener Ableitungen folgte im zweiten Teil des Forschungsprojekts eine eingehende Untersuchung der Generalthematik WLV. Dabei war zentrale Intention dieser Untersuchung, auf Grundlage der erzielten Ergebnisse am Ende auch einen konstruktiven Vorschlag (sc. einen Novellierungsvorschlag auf einfachgesetzlicher Ebene) zu unterbreiten, um anhand eines angepassten Rechtsrahmens mittel- und langfristig in der WLV Schritt für Schritt bestmöglich „… vor mögliche Krisenlagen zu kommen …“.

Bisherige Methoden und Mittel der WLV sind in Österreich, wenn man die lex lata betrachtet, schwergewichtig und traditionell auf Versorgungssicherung ausgerichtet: Das geltende bundesgesetzliche Wirtschaftslenkungs- und Bevorratungsrecht (paradigmatisch: das VerssG 1992 idgF.) wirkt reaktiv und zielt darauf ab, staatliche Abhilfe bei bereits eingetretenen oder doch zumindest zeitnah bevorstehenden Mangellagen betreffend wichtige Versorgungsgüter rechtsförmlich vorzusehen. Diese in der geltenden Rechtslage implementierte reaktive Methodik greift im Lichte der Umfeldveränderungen und multiplen Krisen der letzten Jahre – für sich alleine – zu kurz und wirkt daher – stand alone – nicht mehr zeitgemäß und schon gar nicht zukunftsfähig.

Der Zwischenbefund veranlasste dazu, Überlegungen zur Flankierung des bisherigen – de facto reaktiven – Modells der WLV (Versorgungssicherung) durch neue, tragende Elemente im Sinne präventiv wirkender, systemischer Versorgungssicherheit anzustellen. Dieser Ansatz zu einer methodischen Weiterentwicklung löste naheliegenderweise eine Überblicksanalyse zur rechtlichen Verankerung von Versorgungssicherheit im österreichischen Bundesrecht und EU-Recht aus. Im nächsten Untersuchungsschritt konnten die konzeptiven Ansätze weiter substanziell verfeinert werden – und zwar in Richtung systemischer Resilienz. In Zusammenhalt mit dem wissenschaftlichen Schrifttum ergab sich aus diesen Einsichten die naheliegende Perspektive, bisherige reaktive Ansätze in der WLV (Stichwort: Versorgungssicherung) um eine entscheidende Weichenstellung in Richtung systemischer Versorgungssicherheit bzw. systemischer Resilienz zu ergänzen.

Im abschließenden Untersuchungsschritt sollte ein rechtsvergleichender Blick in die Schweiz, nach Finnland und Japan zur Abrundung der Erkenntnisse beitragen bzw. eventuell zusätzliche Impulse für den aus den gesammelten Erkenntnissen abzuleitenden rechtspolitischen Gestaltungsvorschlag erbringen.

Für die rechtspolitische Stoßrichtung ergab sich letztlich klar: Je nach Szenario internationaler Spannungen wird die österreichische Wirtschaft unterschiedliche Schwächen aufweisen, die vom „Krisenmanagement“ durch adäquate Wirtschaftslenkung „aufgefangen“ werden müssen. Um mit dieser Kontingenz möglicher Szenarien internationaler Spannungen umgehen zu können und um darauf adäquate Antworten der Wirtschaftslenkung zu finden und zu implementieren, sind Methoden der strategischen Vorausschau gemäß State of the Art notwendig, die in einen entsprechenden Prozess eingebettet sind. Anderenfalls kann eine nachhaltige Anhebung systemischer Resilienz bzw. eine Optimierung von Versorgungssicherheit in Österreich nicht erreicht werden. Auf Basis der gewonnenen Erkenntnisse wurde als integrierender Bestandteil des Projekts ein konkreter Novellierungsvorschlag zum Versorgungssicherungsgesetz (VerssG) 1992 idgF. samt Erläuterungen erarbeitet.

Projektleitung:

Technische Universität Wien

Projektpartner:

- Repuco Unternehmensberatung GmbH
- Bundesministerium für Digitalisierung und Wirtschaftsstandort (Bedarfsträger)

Kontakt:

Ao. Univ.-Prof. Dr.iur. Markus Haslinger
TU Wien Forschungsbereich Rechtswissenschaften
Karlsgasse 13/1. OG
1040 Wien
Tel: +43 1 58801 280 111
E-Mail: haslinger@law.tuwien.ac.at
www.institute.tuwien.ac.at/rechtswissenschaften/

WRITE

IT unterstützte Suche und Vergleich von Handschriften

Die Strafverfolgungsbehörden verfügen über eine umfangreiche Sammlung handschriftlicher Dokumente. Dazu gehören z. B. Dokumente, die zu offenen Fällen gehören, sowie Schriftproben von Verdächtigen und Gefangenen. Diese Dokumentensammlungen können jedoch nur begrenzt genutzt werden, da zur Identifizierung eines unbekannten Schreibers, einer unbekannten Schreiberin alle Dokumente manuell von Handschriftexpertinnen bzw. -experten verglichen werden müssen.

WRITE zielt darauf ab, dieses Problem durch die Entwicklung einer IT-basierten Lösung zu lösen, die die Suche nach ähnlichen Handschriften ermöglicht. Auf diese Weise kann die Identifizierung von unbekannten Schreiberinnen bzw. Schreibern durch Handschriftenexpertinnen bzw. -experten beschleunigt werden, da nur eine geringe Anzahl von Dokumenten mit ähnlichen Handschriften manuell verglichen werden muss. Im Gegensatz zu derzeit verfügbaren kommerziellen Lösungen muss bei dem vorgeschlagenen System keine manuelle Klassifizierung der Handschriften im Vorfeld durchgeführt werden. Dies ist zum einen zeitaufwendig und zum anderen fehleranfällig, da es von der subjektiven Meinung der einzelnen Expertin, des einzelnen Experten abhängt.

Die innerhalb des Projekts entwickelte Methodik basiert auf Deep Learning bzw. künstlicher Intelligenz (KI). Dabei werden neuronale Netzwerke mit Hilfe von Datensätzen des Bundeskriminalamts trainiert, um ähnliche Merkmale der Handschrift zu extrahieren und zu gruppieren (Triplet Learning). Ein besonderer Fokus gilt dabei unüberwachten Lernstrategien, um die große Anzahl an Dokumenten, für die teilweise keine Identifizierung vorhanden ist, benutzen zu können. Diese zielen darauf ab, dem Netzwerk eine Metrik beizubringen, um ähnliche Merkmale gruppieren zu können. Der Deskriptor eines Dokumentes setzt sich aus den einzelnen vom Netzwerk extrahierten und beschriebenen Merkmalen zusammen.

Zusätzlich ist ein Fokus des Projektes, den Arbeitsprozess der Handschriftexpertinnen und -experten zu erleichtern. Dazu ist insbesondere die Detektion von Buchstaben bzw. Buchstabenfolgen interessant. Dies wird durch eine KI-gestützte Methodik bewerkstelligt, die aus zwei Teilen besteht: Textdetektion und Texterkennung bzw. Optical Character Recognition (OCR). Während für die Textdetektion ein konventionelles Detektionsmodell verwendet wird, basiert die Buchstabendetektion auf einer neuen Netzwerkarchitektur („Attention“). Die genauen Buchstabenkoordinaten können damit aus Vorhersage des Netzwerks für den Text berechnet werden. Der Vorteil darin besteht, das neuronale Netz ohne genaue Kenntnis der Buchstabenpositionen trainieren zu können.

Die Evaluierung dieser Deep-Learning-basierten Methoden gründet auf drei Datensätzen, die innerhalb des Projektes erstellt werden. Diese setzen sich aus vom Bundeskriminalamt gesammelten Handschriftproben, Dokumenten aus offenen Fällen und Handschriften, die von der TU Wien erstellt wurden, zusammen.

Um die entwickelten Ansätze auch Expertinnen und Experten zur Verfügung stellen zu können, sind diese in einer eigens entwickelten Software mit grafischer Benutzeroberfläche integriert. Der Aufbau und die Funktionalität des User Interfaces wurden mit Mitarbeiterinnen und Mitarbeitern der kriminalpolizeilichen Untersuchungsstelle festgelegt. Diese Software erlaubt eine automatische Suche in zuvor definierten Bereichen. Fragliche Schriftstücke können damit einer Schreiberin, einem Schreiber zugeordnet werden. Dabei werden sogenannte Merkmalsprotokolle mit Hilfe der entwickelten Buchstabendetektion erstellt. Hierzu werden Buchstaben/Zahlen/besondere Buchstabensequenzen der fraglichen Schriften angeordnet und anschließend verglichen. Nach Abschluss des Internvergleichs erfolgt die Gegenüberstellung mit den Vergleichsschriften. Zusätzliche Funktionalitäten nach Bedarf, wie zum Beispiel eine semiautomatisierte Erstellung eines Untersuchungsberichtes, sind in der Software integriert.

Das Projekt wird abgerundet durch eine Analyse der Handschrift, die die Aspekte der Entstehungsbedingungen, Schriftveränderungen durch innere und äußere Umstände und Merkmale der Handschrift beleuchtet. Ein entsprechender Bericht dieser Analyse unterstützt die Entwicklung einer zielgerichteten Methode, um die Herausforderungen des Handschriftenvergleichs besser abbilden zu können. Zusätzlich wird dies anhand von Beispielen des Bundeskriminalamts untersucht.

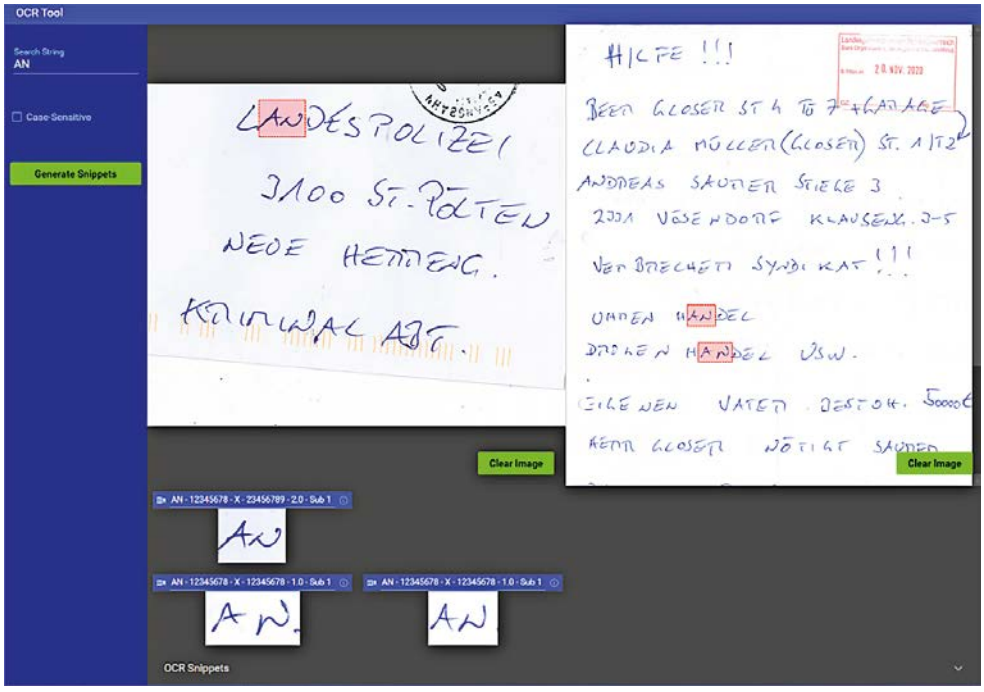


Abb.: Grafische Benutzeroberfläche: Suche nach der Buchstabenfolge „AN“

Projektleitung:

Technische Universität Wien

Projektpartner:

- Bundesministerium für Inneres - Bundeskriminalamt, Abt 6, Büro für Kriminaltechnik
- cogvis software und consulting GmbH
- Elisabeth Charkow, Dipl. Graphologin ÖGS und Schriftsachverständige

Kontakt:

Univ.-Prof. DI Dr. Robert Sablatnig
TU Wien, Computer Vision Lab, Institute of Visual Computing & Human-Centered Technology
Favoritenstr. 9/193–1
1040 Wien
Tel: +43 1 58801 193 161
E-Mail: sab@cvl.tuwien.ac.at
www.cvl.tuwien.ac.at/