

Sicher. Innovativ. Erfolgreich.

*Erfolgsgeschichten aus
der Österreichischen
Sicherheitsklammer*



KIRAS

Zivile Sicherheitsforschung

FORTE

Verteidigungsforschung

K-PASS

Cybersicherheitsforschung



Von der Forschung in den Markt:
10 Projekte der Sicherheitsklammer

EXPERTENINTERVIEW

Dr. Ralph HAMMER***Warum ist Sicherheitsforschung heute wichtiger denn je – und welche Rolle spielt sie für den Wirtschafts- und Innovationsstandort Österreich?***

Sicherheitsforschung war und ist von gleichbleibender Bedeutung, da sie nur wirksam ist, wenn sie rechtzeitig vor Krisen und anderen sicherheitsrelevanten Ereignissen gefördert wird. Von der Idee bis zur einsatzfähigen Anwendung vergehen meist 5 bis 7 Jahre. Daher müssen Bedarfsträger wie Blaulichtorganisationen, Militär und Betreiber Kritischer Infrastrukturen künftige Herausforderungen frühzeitig erkennen, damit sie im Rahmen der Forschungsförderung des Bundesministeriums für Finanzen (BMF) unterstützt werden können. So stehen im Bedarfsfall Produkte und Dienstleistungen „Made in Austria“ zur Verfügung und schaffen zugleich wirtschaftlichen Mehrwert.

Welche Bedeutung haben die Forschungsprogramme der Sicherheitsklammer für den Innovationsstandort Österreich?

Die Programme der Sicherheitsklammer adressieren mit ihrer Ausrichtung und ihrem Budget gezielt einen Innovationsbereich, der als „Querschnittsmaterie“ ohne spezifische Fördermaßnahmen kaum strukturiert und erfolgreich angesteuert werden kann. Die meisten europäischen Staaten verfügen über keine mit KIRAS, FORTE oder K-PASS vergleichbaren Instrumente auf staatlicher Ebene. Das verschafft Österreich sicherheitspolitisch und wirtschaftlich einen wichtigen Wettbewerbsvorteil.

Was macht die österreichische Sicherheitsforschung und die Sicherheitsklammer im internationalen Vergleich besonders?

Das zivile Sicherheitsforschungsprogramm KIRAS machte Österreich 2006 zum ersten Land Europas mit einem Programm dieser Art. Durch die verpflichtende Einbindung von Bedarfsträgern, Forschungseinrichtungen, Unternehmen sowie den Geistes-, Sozial- und



Ministerialrat
Dr. Ralph HAMMER
Leiter

Bundesministerium für Finanzen
Sektion VI - Bergbau
Stabsstelle f. Sicherheitsforschung und
Technologietransfer

ralph.hammer@bmf.gv.at
+43 1 514 335 061 30
www.kiras.at

Kulturwissenschaften (GSK) entstand ein wegweisendes Innovationsmodell, das vielfach auf EU-Ebene übernommen wurde. Ein weiteres Alleinstellungsmerkmal ist der Förderkoordinationsrahmen der Österreichischen Sicherheitsklammer: Das BMF koordiniert, finanziert und stimmt sowohl die zivile (Cyber) Sicherheits- als auch die nationale Verteidigungsforschung thematisch aufeinander ab. Dadurch werden Stärken gebündelt und die unterschiedlichen Erwartungen der beteiligten Akteure wirksam aufeinander abgestimmt.

IMPRESSUM

Medieninhaber und Verleger: Media Guide

Herausgeber: Jonas Buchegger, jbuchegger@myguides.at

Fotos: AdobeStock, Freepik, Vertragspartner

Grafik: Agentur be-design, Karin Schön, office@be-design.at, www.be-design.at

Das Medium „Erfolgsgeschichten aus der Österreichischen Sicherheitsklammer“ erscheint in Kooperation mit dem Bundesministerium für Finanzen. Das vorliegende Medium wurde von Expertinnen und Experten begutachtet und für gut befunden. Dennoch erfolgen alle Angaben ohne Gewähr. Weder die Autorinnen und Autoren oder die Expertinnen und Experten, noch der Verlag können für eventuelle Nachteile oder Schäden, die aus den im Heft gegebenen Hinweisen resultieren, eine Haftung übernehmen. Veröffentlichung oder teilweise Veröffentlichung nur mit schriftlicher Genehmigung des Verlages.

Anzeigenannahme: Falls Sie mehr über Kooperationsmöglichkeiten wissen möchten, fordern Sie bitte nähere Informationen an: MediaGuide Verlag, Tel. 0664/5271172, E-Mail: jbuchegger@myguides.at.

Herzlichen Dank an alle, die zur Vollständigkeit und zum Gelingen durch ihre Mitarbeit beigetragen haben.

INHALTSVERZEICHNIS

Infografik Sicherheitsklammer	3
Fact Sheet Sicherheitsforschung	4
HiProtect®	6
Backbone	8
Bäckerei Deiser	10
Fake-Shop Detector	12
DeFiTrace	14
CESARE	16
Minerva	18
AIT - AttackBed und Cyber Range	20
KI-SecAssist	22
Desinfact	24

Sicherheitsklammer Impact Level – Forschungserfolg messbar machen

Wie gelingt der Weg von einer guten Idee zu einer erfolgreichen Anwendung? Das Sicherheitsklammer Impact Level macht die Entwicklung eines Projekts auf einen Blick sichtbar. Anhand von sieben Entwicklungsstufen – von der validierten Forschungsidee bis hin zur erfolgreichen Skalierung am Markt – wird nachvollziehbar, wie weit ein Projekt auf seinem Weg zur praktischen Wirkung bereits fortgeschritten ist.

Projektleiter:innen stufen ihre Projekte allgemein und in vier zentralen Wirkungsdimensionen ein: Sicherheit, gesellschaftlicher Nutzen, Exportpotenzial und wirtschaftliches Potenzial. Die Selbsteinschätzung erfolgt auf einer Skala von 1 bis 7 und schafft eine einheitliche Vergleichsbasis zwischen den vorgestellten Projekten.

Das Sicherheitsklammer Impact Level versteht sich dabei nicht als wissenschaftliche Bewertung, sondern als praxisorientiertes Instrument, das Entwicklungsstand und Wirkungspotenzial transparent und vergleichbar darstellt. So erhalten Leserinnen und Leser einen schnellen Überblick darüber, welchen Reifegrad ein Projekt erreicht hat und welches Potenzial es für Wirtschaft, Gesellschaft und die Sicherheitsforschung bietet.

SICHERHEITSKLAMMER IMPACT LEVEL

Von der Idee zur Wirkung. MESSBAR. ZUKUNFTSWEISEND. INNOVATIV.



	1	2	3	4	5	6	7
 SICHERHEIT	☐	☐	☐	☐	☐	☐	☐
 GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☐	☐	☐
 EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☐
 WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☐	☐	☐

Fact Sheet

Sicherheitsforschung

DIE 3 FORSCHUNGSPROGRAMME:

Was ist die Sicherheitsklammer?		DIE 3 FORSCHUNGSPROGRAMME:		
Die österreichische Sicherheitsklammer		1	2	3
		KIRAS	FORTE	K-PASS
> Das in 2006 etablierte zivile Sicherheitsforschungsprogramm KIRAS, das seit 2018 laufende Verteidigungsforschungsprogramm FORTE sowie das 2023 eingeführte digitale (Cyber-)Sicherheitsforschungsprogramm Kybernet-Pass (K-PASS) bilden gemeinsam die österreichische „Sicherheitsklammer“, in der sämtliche sicherheitspolitische Forschungsförderungen des Bundes konzentriert werden. > Förderinstrumente: Kooperative F&E-Projekte oder F&E-Dienstleistungen. > 540 Projekte* mit rd. € 196 Mio. bereits gefördert. > FFG wurde mit dem Programmmanagement beauftragt.	Anzahl der Ausschreibungen 2006-2024	49	7	2
	Anzahl eingereichter Projekte	1.013	204	46
	Anzahl genehmigter Projekte	415	82	24
	Verhältnis Projekte genehmigt : abgelehnt	~ 1 : 2,43	~ 1 : 1,49	~ 1 : 2
	Projekt-gesamtkosten	~ 230 Mio. €	~ 75,9 Mio. €	~ 26,3 Mio. €
	Förderung	~ 148,2 Mio. €	~ 35,4 Mio. €	~ 11,3 Mio. €
	Bisher beantragte Förderung (gesamt)	~ 349,4 Mio. €	~ 97,6 Mio. €	~ 23,7 Mio. €

Generelle Aussagen zur österreichischen Sicherheitswirtschaft (ohne Verteidigungssektor): € 2,8 Mrd. Bruttowertschöpfung und rd. 41.500 Beschäftigte. Der Produktionsmultiplikator liegt bei rd. 1,53 (vergleichbar mit der Bauwirtschaft)**).

^{*)} Inkl. geförderter „Innovation AKUT“ Projekte der Ausschreibungen 2023/24 und 2024/25
^{**)} Ergebnisse des Sicherheitssatellitenkontos 2022

HiProtect®

Entwicklung eines neuartigen Leichtbau-Materialverbundes mit ballistischen und selbstheilenden Schutzeigenschaften



Die Abbildung rechts zeigt den Aufbau, bestehend aus vier nebeneinander angeordneten Einzelelementen.

Ballistische Schutzeinrichtungen militärischer Einheiten sollen einfach zu transportieren und rasch aufbaubar sein. Faserverstärkte Hochleistungsverbundkunststoffe sind für derartige Leichtbauanwendungen prädestiniert, wobei die erforderliche Durchschusssicherheit nur durch die Entwicklung geeigneter Werkstoff- und Bauteilstrukturen zu erreichen ist.

Das direkte Ergebnis des Forschungsprojektes ist ein funktionsfähiger Prototyp eines modularen, ultraleichten Schutzsystems, das bei einem Flächengewicht von 4,9 kg/m² Geschossenergien bis mindestens 1600 J absorbieren kann. Dies entspricht in etwa dem Beschuss mit einem Sturmgewehr aus 50-100m Entfernung. Die Elemente werden dabei eben und platzsparend übereinander gestapelt zum Bedarfsträger geliefert. Dieser kann sie aufspannen und zu einer großflächigen Schutzstruktur zusammensetzen. Die Abbildung links zeigt einen solchen Aufbau, bestehend aus vier Einzelelementen. Auf der weißen Vorderseite ist ein Einschussloch in der Schutzplatte zu erkennen.

Neben dem Schutz von Equipment und Infrastruktur kann das modulare System mit seinem Wirkprinzip auch zum Schutz von Fahrzeugen angewendet werden. Zusammen mit der Firma Liebherr aus Telfs in Tirol wurde ein Teleskopplader als Demonstratorfahrzeug umgebaut.



VORTEILE:

- > Keine Verstärkung des Chassis notwendig
- > Große Freiheit beim Design, kein Aufbau aus Plattenmaterial notwendig
- > Betriebserlaubnis kann beibehalten werden
- > Aufrüstung im Feld in kurzer Zeit möglich
- > Das relativ geringe Mehrgewicht der Schutzlösung beeinträchtigt das Fahrverhalten und die Schwerpunktage der Maschine nicht negativ
- > Die Arbeitsmaschine kann im Alltag ohne Einschränkungen genutzt werden. Im Kriseneinsatz arbeitet das Personal dann mit der gewohnten Maschine.
- > Beschädigte Schutzelemente können einzeln, schnell und ohne schweres Gerät ausgetauscht werden.

EXPERTENINTERVIEW

Dr.-Ing. Jochen Schmidt

Welche wirtschaftlichen Potenziale sehen Sie für HiProtect und die Weiterentwicklung Hi2Protect im internationalen Sicherheits- und Leichtbaumarkt?

Das wirtschaftliche Potenzial von HiProtect und Hi2Protect liegt vor allem in der Verbindung von hochwirksamem Schutz und konsequentem Leichtbau. Diese Kombination wird international stark nachgefragt – sowohl im Verteidigungsbereich als auch für zivile sicherheitskritische Anwendungen.

Besonders in der kritischen Infrastruktur bieten leichte Composite-Lösungen Vorteile, da sie Montageaufwand, statische Anforderungen und Betriebskosten reduzieren.

Großes Potenzial sehen wir zudem im Mobilitätssektor – etwa bei Spezialfahrzeugen oder maritimen Anwendungen, sowie bei persönlicher Schutzausrüstung.

Inwiefern könnte die Kombination aus ballistischen und selbstheilenden Eigenschaften langfristig Kosten reduzieren?

Die Kombination aus ballistischen und selbstheilenden Eigenschaften bietet großes wirtschaftliches Potenzial über den gesamten Lebenszyklus eines Systems.

Das Hi2Protect System kann Impactschäden verschließen, so sind diese nach außen hin nicht offensichtlich erkennbar und gleichzeitig wird das Schutzmaterial weiterhin gegen Umwelteinflüsse geschützt.

Dadurch reduzieren sich Wartungsaufwand, Inspektionsintervalle und Ersatzteilkosten deutlich. Besonders bei kritischer Infrastruktur ist das relevant, da Ausfallzeiten oft höhere Kosten verursachen als das Bauteil selbst.

Welche Chancen bietet die in Österreich entwickelte Technologie für den Wirtschaftsstandort selbst?

Die in Österreich im FORTE-Forschungsförderungsprogramm entwickelte Technologie bietet große Chancen für den Wirtschaftsstandort – technologisch, wirtschaftlich und strategisch. Besonders im Bereich intelligenter



Dr.-Ing. Jochen Schmidt
Hintsteiner Group

j.schmidt@hintsteiner.at
+43 3864 23 36 - 54
www.hintsteiner-group.com

STATEMENT DEVELOPER:

Liebherr / Michael Hagner
Key Account Manager Defense/
Product Manager Telescopic handler
Michael.Hagner@liebherr.com



Für das Liebherr-Werk Telfs als Hersteller von Teleskopladern und Planierraupen bietet der Hi2Protect Schutz viele Vorteile. Wir haben durch diesen leichten Schutz die Möglichkeit unseren Kunden ein Serienfahrzeug anzubieten, welches nicht aufwendig mit stärkeren Achsen oder anderen Komponenten angepasst werden muss, um eine geschützte Kabine tragen zu können. So hat der Kunde den großen Vorteil, dass er nicht nur vom Preis einer Serienmaschine profitiert, sondern auch von der Ersatzteilverfügbarkeit einer Maschine, die bereits tausendfach im Einsatz ist.

Leichtbau- und Schutzsysteme kann das Land international eine starke Position einnehmen. Technologien wie HiProtect und Hi2Protect stärken die Unabhängigkeit Europas bei sicherheitsrelevanten Hochleistungsmaterialien und reduzieren Abhängigkeiten. Gleichzeitig sehen wir erhebliches Exportpotenzial, da der internationale Markt für Sicherheits-, Infrastruktur- und Mobilitätslösungen stark wächst. Langfristig kann sich Österreich dadurch als europäischer Entwicklungs- und Produktionsstandort für moderne Schutz- und Composite-Technologien weiter etablieren. ♦

SICHERHEITS- KLAMMER

IMPACT LEVEL

7

	1	2	3	4	5	6	7
 SICHERHEIT	☐	☐	☐	☐	☐	☒	☐
 GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☒	☐	☐
 EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☒
 WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☐	☒	☐

BACKBONE

ULTRASICHERES END-USER-DEVICE

EXPERTENINTERVIEW mit **PHILIPP LECHNER**, CEO von MUSE Electronics

Welche konkreten Anwendungsfälle Ihres BACKBONE-Tablets haben sich bisher in der Praxis als besonders wirkungsvoll erwiesen, und wie hebt es sich von anderen vergleichbaren Produkten ab?

Lassen Sie mich das an zwei konkreten militärischen Szenarien verdeutlichen, die zeigen, warum BACKBONE kein gewöhnliches Tablet ist. Das Wort Single-Device trifft es schon besser: ein einziges Device, welches es ermöglicht durch strikte physikalische Datentrennung in mehreren Sicherheits-Domänen zu arbeiten.

Stellen Sie sich einen Aufklärungsoffizier in einem multinationalen NATO-Einsatz vor. Er arbeitet gleichzeitig mit „Mission Secret“-Daten der gemeinsamen Kommandostruktur und mit „National Confidential“-Informationen seines Heimatlandes – Daten, die unter keinen Umständen vermischelt werden dürfen. Mit BACKBONE trägt er ein Single-Device, das die Daten beider Domänen physikalisch getrennt bearbeitet und speichern kann. Keine Lösung auf Software-Ebene – sondern echte, hardwareseitige Trennung. Das ist ein Paradigmenwechsel.

Das zweite Szenario ist ein Spezialkräfte-Einsatz in unwegsamem Gelände. Hier geht es nicht nur um Datensicherheit, sondern auch um absolute Zuverlässigkeit unter physischen Extrembedingungen. Das Gerät muss funktionieren – bei -20 Grad, im Regen, nach



Mag. Philipp Lechner
CEO von MUSE Electronics

contact@backbone.io
www.backbone.io

einem Sturz. Und es muss garantieren, dass im Fall einer Kompromittierung keine missionskritischen Daten abgegriffen werden können. BACKBONE erkennt Manipulationsversuche automatisch und löst sofort Sicherheitsroutinen aus.

Was uns von anderen Produkten unterscheidet: Vergleichbare Geräte versuchen Sicherheit mit Software zu lösen – das ist strukturell angreifbar. Wir lösen es auf Hardware-Ebene. Das ist kein gradueller Unterschied, das ist ein fundamentaler. Mag. Wolfgang Hacker, CTO der Direktion 6 IKT und Cyber, bringt es auf den Punkt: Ein gehärtetes Endgerät, das über verschiedene Kommunikationskanäle verfügt, in mehreren Sicherheitsdomänen einsetzbar ist und mit bestehender Ausstattung kompatibel bleibt, birgt enormes Potenzial für die zukünftige IKT-Architektur im Einsatz.

Wo liegt aus Ihrer Sicht das größte wirtschaftliche Potenzial Ihrer Lösung – eher in der Skalierung bestehender Märkte oder in der Erschließung völlig neuer Anwendungsfelder?

Beides – aber in unterschiedlichen Zeithorizonten. Kurzfristig liegt das größte Potenzial klar in der Skalierung bestehender Märkte. Europa rüstet auf, die NATO-Mitgliedstaaten erhöhen ihre Verteidigungsbudgets massiv, und der Bedarf an vertrauenswürdiger, europäischer Technologie war noch nie so groß wie heute. Wir sind im Rahmen des European Defence Funds als Konsortialführer gut positioniert, um genau diesen Moment zu nutzen.

Mittelfristig aber sehe ich enormes Potenzial in neuen Anwendungsfeldern – und der Treiber dahinter ist klar: Cyberbedrohungen werden nicht weniger, sie werden

breiter, gezielter und professioneller. Kritische Infrastruktur, Energieversorgung, Justiz, Behörden – all diese Bereiche sind längst im Visier staatlicher und nichtstaatlicher Angreifer. Der Bedarf an Lösungen, die auf Hardware-Ebene sicher sind, wächst damit weit über den militärischen Sektor hinaus.

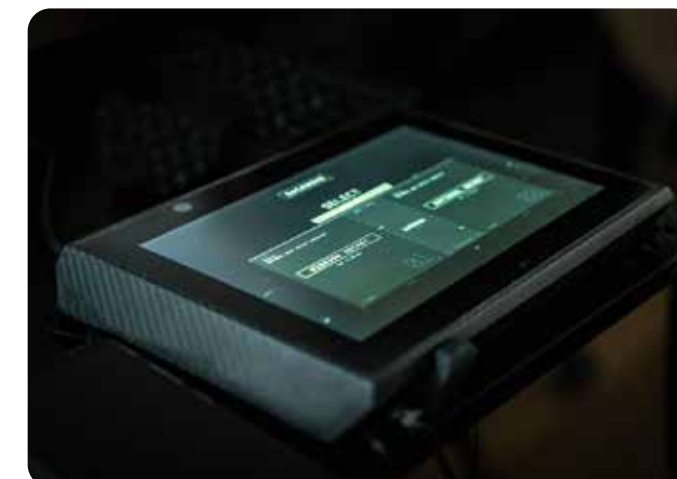
Überall dort, wo bisher mehrere Geräte nötig waren oder wo sensible Daten auf unzureichend gesicherten Endgeräten verarbeitet wurden, kann BACKBONE als einheitliche, vertrauenswürdige Plattform eingesetzt werden. BACKBONE ist nicht auf Soldat:innen im Feld beschränkt – es ist eine Antwort auf eine gesamtgesellschaftliche Herausforderung.

Und das führt mich zu einem Punkt, der mir besonders wichtig ist: Europa braucht eine autonome Hardware-Industrie. Wir können nicht einerseits digitale Souveränität fordern und andererseits die Geräte, auf denen unsere sensibelsten Daten laufen, aus Drittstaaten beziehen. Systemrelevante Industrien – und dazu gehört die Hardware-Industrie zweifellos – müssen in Europa entstehen und wachsen. BACKBONE ist dafür ein konkretes Beispiel: entwickelt und gebaut in Österreich, mit dem Anspruch, europäischer Standard zu werden.

Welche nächsten Schritte sind entscheidend, um BACKBONE großflächig am Markt zu etablieren, und welche Rolle spielen dabei Partnerschaften oder internationale Expansion?

Der entscheidende Schritt ist der aktuell laufende Marktstart und die dahinter liegenden ersten Kundenauslieferungen. Das ist die Grundlage für alles weitere. Parallel dazu ist der gezielte Aufbau eines Partnernetzwerks aus spezialisierten Systemintegratoren absolut zentral. BACKBONE muss in bestehende Sicherheitsarchitekturen eingebettet werden können – das gelingt nur mit langjährigen Partnern.

Zur internationalen Expansion: Unser Fokus liegt auf Europa, den NATO-Staaten und deren Partnerstaaten – also genau jenen Ländern, die gerade aktiv daran arbeiten, ihre Verteidigungsfähigkeiten auszubauen und ihre technologische Abhängigkeit von nicht-euro-



päischen Herstellern zu reduzieren. Dieser Moment ist entscheidend: Beschaffungsentscheidungen, die heute getroffen werden, prägen die Sicherheitsarchitektur der nächsten Dekade.

Überall dort, wo Streitkräfte oder Behörden auf interoperable, sichere Endgeräte angewiesen sind, ist BACKBONE eine überzeugende Antwort – nicht trotz seiner europäischen Herkunft, sondern gerade deswegen. Vertrauenswürdigkeit beginnt bei der Frage, wo und von wem ein Gerät gebaut wurde.

Die Vision ist, dass BACKBONE der selbstverständliche Standard für sicheres mobiles Arbeiten in Hochrisikobereichen wird – entwickelt und gebaut in Österreich, gedacht für Europa und seine Partner. ♦

FACTS:

BACKBONE wird von MUSE Electronics in Wien & Budapest entwickelt und gefertigt. Das Unternehmen wird von CEO Philipp Lechner geführt, durch das österreichische Verteidigungsforschungs-Förderprogramm FORTE sowie den European Defence Fund unterstützt und durch eine Serie-A Finanzierung von Sparring Capital Partners gestärkt.



SICHERHEITS-KLAMMER

IMPACT LEVEL

6

	1	2	3	4	5	6	7
 SICHERHEIT	☐	☐	☐	☐	☒	☐	☐
 GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☒	☐	☐
 EXPORT POTENTIAL	☐	☐	☐	☐	☒	☐	☐
 WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☒	☐	☐

Bäckerei Deiser

Dosenbrot für die Krisenvorsorge



VORTEILE:

- > mittlerweile 5 Brotsorten und 2 Kuchen im Dosen-Sortiment (Roggenvollkornbrot, Roggenmischbrot, Vollkornmischbrot mit Sonnenblumenkernen, Eiweißbrot, Hanfbrot, Schokokuchen mit Schokostückchen, Zitronenkuchen)
- > lange haltbar:
MHD von 10 Jahren ab Produktionsdatum
- > natürliche Zutaten: Brote mit Sauerteig, ohne Hefezusatz und vegan, Roggenvollkornbrot – weizenfrei; die Kuchen ohne Palmöl
- > sofort verzehrfertig
- > Psychologisch entlastend, weil ein gesicherter Lebensmittelvorrat die Selbstversorgung in Krisen verbessert
- > Weißblechdose mit Bisphenol (BPA) freier Innenbeschichtung
- > praktisch für unterwegs
- > autarker Betrieb, der in einer Krisensituation – wie einem Black Out – weiter produzieren kann. Wobei in so einem Fall nur frisches Brot für die Bevölkerung produziert werden wird.

Die Bäckerei Deiser wurde 1964 gegründet und war ursprünglich ein typisches Wiener Familienunternehmen mit eigenem Geschäftslokal sowie einem vielfältigen Sortiment aus Brot, Gebäck und Süßspeisen.

Im Jahr 1989 übernahm Christian Deiser den Betrieb und schlug gezielt neue Wege ein.

Neben der Spezialisierung auf Sauerteigbrote setzte er auf Rohstoffe, die zu mindestens 90% aus Österreich stammen. Gleichzeitig legte er großen Wert auf Energieeffizienz: Zunächst wurde am Standort in Wien ein System zur Wärmerückgewinnung umgesetzt, bevor 2017 eine eigene energieautarke Produktionshalle in Baden bei Wien in Betrieb genommen wurde.

Anfang 2019 suchte die Stabsstelle für die Sicherheitsforschung und Technologietransfer gemeinsam mit der Forschungsförderungsgesellschaft (FFG), der Wirtschaftskammer Österreich (WKÖ, Bereich Lebensmittel) sowie der Bäckerinnung einen österreichischen Bäckereibetrieb mit freien Kapazitäten, um die Produktion von Dosenbrot wieder im Inland aufzunehmen.

Bis Mitte der 1970er-Jahre wurde Dosenbrot bereits von einem Wiener Betrieb hergestellt; das Ziel war es, die Eigenversorgung in Österreich wieder zu etablieren. Es handelte sich dabei nicht um ein Förderprojekt der österreichischen Sicherheitskammer, sondern um die Umsetzung individueller Kundenaufträge.

Da in der Branche bekannt war, dass die Bäckerei Deiser über eine neu errichtete Produktionshalle verfügt, ihren Strom selbst erzeugt, speichern kann und sogar Überschüsse ins Netz einspeist sowie freie Kapazitäten besitzt, erwies sie sich als idealer krisenfester Partner für die Wiederaufnahme der Dosenbrotproduktion.



EXPERTENINTERVIEW

MMSt Christian P. Deiser

Welche Rolle kann Dosenbrot in der privaten Krisenvorsorge und bei der Sicherstellung der Grundversorgung in Notlagen spielen?

Dosenbrot kann in der privaten Krisenvorsorge eine wichtige Rolle spielen, da es als haltbares, sofort verzehrbare Grundnahrungsmittel unabhängig von Strom, Kühlung oder Kochen verfügbar ist.

Während frühere Generationen selbstverständlich Vorräte anlegten, hat die heutige Rund-um-die-Uhr-Versorgung oft zu einer trügerischen Sicherheit geführt. In Krisensituationen wie Stromausfällen, Lieferengpässen oder Naturereignissen zeigt sich jedoch, wie wichtig eigene Vorsorge ist.

Dosenbrot kann zwar keine vollständige Ernährung ersetzen, aber in Kombination mit Wasser, Aufstrichen und Konserven die Grundversorgung über Tage oder Wochen sichern und Versorgungslücken überbrücken. Eine breitere Verfügbarkeit im Handel würde den Zugang erleichtern und mehr Menschen zur Vorsorge befähigen.

Zudem ist Dosenbrot auch im Alltag sowie bei Outdoor-Aktivitäten wie Camping oder Wandern eine praktische und zuverlässige Reserve.

Als Teil der kritischen Infrastruktur: Wie stellt Ihre Bäckerei – insbesondere auch durch die Produktion von Dosenbrot – eine resiliente und energieautarke Betriebsführung sicher?

Unsere Bäckerei ist seit 2018 vollständig energieautark. Den gesamten Strombedarf decken wir zu 100 % über eine eigene Photovoltaikanlage (182 kWp) mit Speicherlösungen. Ergänzend betreiben wir ein Biomasseheizwerk (400 kW), das unsere Thermoöl-Backöfen mit Wärme versorgt; das benötigte Waldhackgut stammt aus der unmittelbaren Region. Als Teil der kritischen Infrastruktur setzen wir konsequent auf re-



Team Deiser
Bäckerei Deiser

team@deisers.com
www.deisers.com

gionale Versorgungsketten: Mindestens 90 % unserer Rohstoffe kommen aus Österreich. Unser Getreide beziehen wir von niederösterreichischen Landwirten über eine Mühle im Nachbarort. Im Krisenfall können wir das Getreide selbst abholen, vor Ort vermahlen und unmittelbar zu Brot weiterverarbeiten. So stellen wir eine resiliente, energieunabhängige Produktion und eine verlässliche Versorgung – auch in Ausnahmesituationen – sicher.

Welche Chancen ergeben sich daraus für österreichische Produzenten wie Deiser, auch auf internationalen Märkten eine Vorreiterrolle einzunehmen?

Die zunehmenden globalen Krisen und die wachsende Bedeutung von Versorgungssicherheit eröffnen österreichischen Produzenten wie uns klare Chancen – insbesondere, wenn es gelingt, die nationale und internationale Sichtbarkeit zu steigern.

Unsere autarke Produktion ermöglicht verlässliches und unabhängiges Handeln. In Verbindung mit hohen Qualitätsstandards und der starken Positionierung „in Österreich hergestellt“ als glaubwürdige Alternative zu fragilen globalen Lieferketten entsteht das Potenzial, international eine Vorreiterrolle einzunehmen. ♦

SICHERHEITS-KLAMMER

IMPACT LEVEL
7

	1	2	3	4	5	6	7
SICHERHEIT	☐	☐	☐	☐	☐	☒	☐
GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☐	☐	☒
EXPORT POTENTIAL	☐	☐	☐	☐	☐	☒	☐
WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☐	☐	☒

Fake-Shop Detector

Fake-Shop Detector

Keine Chance für Online-Betrug:
Warnung vor Fake-Shops mit einer
Genauigkeit von mehr als 99 %

Cyberkriminalität stellt ein wachsendes Problem für Konsument:innen in Österreich dar. Allein die österreichische Melde- und Informationsplattform Watchlist Internet erhält jährlich tausende Meldungen von Konsument:innen zu Betrugsfällen — 2025 waren es knapp 17.000. Gleichzeitig listet die Watchlist mit Stand Juni 2026 rund 25.000 Fake-Shops. Wurde bezahlt, ist das Geld oft verloren. Umso wichtiger ist die Betrugsbekämpfung durch Prävention. Dafür wurde mit dem Fake-Shop Detector ein KI-basiertes Tool entwickelt, das Konsument:innen während des Online-Einkaufs schützt und in Echtzeit warnt. Das im Browser installierte Plugin zeigt die Bewertung eines Shops in Form eines Ampelsystems an und wird von über 10.000 Benutzer:innen täglich verwendet, um sicher im Internet einzukaufen.

Der Fake-Shop Detector verhindert Betrugsfälle frühzeitig, fördert einen sicheren Online-Handel und leistet einen wichtigen Beitrag zur Prävention, indem Opfer vor finanziellen Schäden geschützt und betrügerische Fake-Shops schneller erkannt werden. Die Forschungsarbeit zur Erkennung von Fake-Shops mit Hilfe von Künstlicher Intelligenz wurde maßgeblich von AIT Austrian Institute of Technology, dem Österreichischen Institut für angewandte Telekommunikation (ÖIAT) und dem oberösterreichischen IT-Unternehmen X-Net Services GmbH durchgeführt und im Rahmen mehrerer Programme durch das Sicherheitsforschungsprogramm KIRAS der österreichischen Sicherheitsklammer gefördert.



VORTEILE:

- > Genauigkeit von über 99 % in der Erkennung von Fake-Shops
- > Ausgezeichnet als das wirksamste Sicherheitsprodukt gegen Internet-Fake-Shops 2024 und mit dem Staatspreis für Digitalisierung 2023 Betrugsbekämpfung durch Prävention
- > Stetiges Re-Learning neuer „Angriffsmuster“
- > KI ermöglicht eine zusätzliche ‚Sichtweise‘ für Expert:innen
- > Förderung der digitalen Kompetenz der User:innen mit Community Effekt: „schütze dich und andere“
- > Echtzeitanalyse durch KI und sofortige Anzeige mittels Ampelsystem
- > Implementierung, Betreuung und Hosting in Österreich
- > Schutz der Privatsphäre und keine Speicherung von personenbezogenen Daten

STATEMENT

Nikolaus Dürk
(Geschäftsführer und Gründer von X-Net)

Mit dem Fake-Shop Detector wurde eines der weltweit besten KI-Systeme im Bereich der Betrugsprävention entwickelt. Bei einem flächendeckenden Einsatz in Österreich können die Betrugsquote wesentlich gesenkt und ein Abgang von hunderten Millionen Euro jährlich vermieden werden. Durch diese modernen Möglichkeiten der KI gesteuerten Präventionsarbeit werden die österreichischen Bürger:innen geschützt, die Verwaltung entlastet und ein enormes Potential wieder dem Markt bereitgestellt, Geld das sonst irgendwo außerhalb unseres EU-Wirtschaftsraums abwandert.

STATEMENT

Bernhard Jungwirth
(Geschäftsführer von Österreichisches Institut für angewandte Telekommunikation, kurz ÖIAT)

Jedes Jahr wenden sich tausende Konsument:innen mit Betrugsfällen an die Watchlist Internet. Mit dem Fake-Shop Detector schützen wir genau diese Menschen: Das Plugin warnt Konsument:innen in Echtzeit und direkt im Browser, die dabei neu entdeckten betrügerischen Shops fließen wiederum in die Warnlisten der Watchlist Internet ein. So schützt jede einzelne Nutzerin und jeder einzelne Nutzer nicht nur sich selbst, sondern hilft mit, um andere schneller warnen zu können. Wirksamer Konsumentenschutz entsteht an genau dieser Schnittstelle zwischen verlässlicher Information, niederschwelliger Technik und einem Netzwerk, das mit jeder Meldung besser wird.

STATEMENT

Helmut Leopold
(Head of Center for Digital Safety & Security, AIT Austrian Institute of Technology)

Der Fake-Shop Detector zeigt, wie verantwortungsvoll entwickelte Künstliche Intelligenz einen konkreten gesellschaftlichen Mehrwert schaffen kann. Durch die Kombination aus KI gestützter Analyse und kontinuierlicher Qualitätssicherung durch Expert:innen gelingt es, Onlinebetrug frühzeitig zu erkennen und Konsument:innen präventiv zu schützen. Die mehrfachen Auszeichnungen – darunter der Staatspreis Digitalisierung 2023 – sowie die jüngste unabhängige Evaluierung durch AV Comparatives, bei der der Fake-Shop Detector als leistungsstärkste österreichische Lösung im internationalen Vergleich bestätigt und mit einem entsprechenden Zertifikat ausgezeichnet wurde, unterstreichen den Anspruch des AIT, vertrauenswürdige Technologien mit realer Wirkung für Gesellschaft und Wirtschaft zu entwickeln.

SICHERHEITS- KLAMMER



	1	2	3	4	5	6	7
 SICHERHEIT	☐	☐	☐	☐	☐	☐	☒
 GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☐	☐	☒
 EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☒
 WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☐	☒	☐

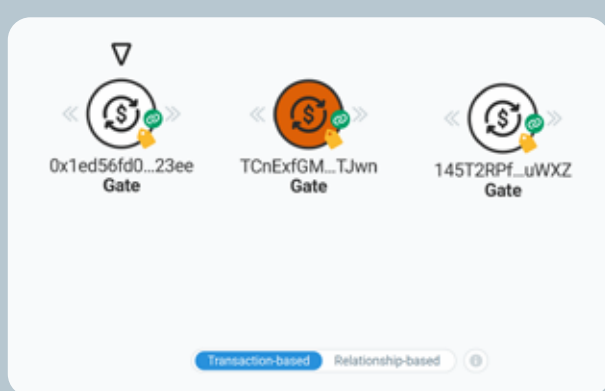
DeFiTrace

Wie sich illegale Geldflüsse durch dezentrale Finanzsysteme zurückverfolgen lassen

Dezentrale Finanzsysteme (DeFi) wickeln Finanzgeschäfte über Blockchains ab, ohne Banken oder andere zentrale Vermittler. Das erschwert die Verfolgung illegaler Zahlungsströme, und klassische, manuelle Ermittlungsmethoden stoßen dabei an ihre Grenzen. Eine im Projekt erstellte Ausgangsstudie dokumentierte über 1.100 Cybercrime-Fälle mit mehr als 30 Milliarden US-Dollar Schaden zwischen 2017 und 2022. Im Projekt DeFiTrace entstanden mehrere datengetriebene Analysemethoden, die in die GraphSense-Untersuchungsplattform eingeflossen sind. Eine neu entwickelte Methode zur Cross-Chain-Analyse identifizierte über 1,5 Millionen Krypto-Adressen mit Verbindungen zu mehreren Blockchains. Eine quantitative Governance-Analyse zeigte, dass in über 20 Prozent der DeFi-Projekte zumindest eine wichtige Entscheidung ausschließlich von zentralen Akteur:innen getroffen wurde. Das automatisierte QuickLock-System verfolgt verdächtige Zahlungsströme und ersetzt mühsame Einzelrecherche. In enger Zusammenarbeit mit österreichischen Behörden wurden diese Methoden entwickelt und Ermittlerinnen und Ermittler geschult, die Inhalte sind fest in der Ausbildung der Bundesfinanzakademie verankert.

VORTEILE:

- > Cross-Chain-Tracing über Blockchain-Grenzen hinweg (UTXO- und Account-Modell)
- > Automatisierte Massenanalyse statt manueller Einzelrecherche (QuickLock)
- > In die produktive GraphSense-Plattform integriert und damit sofort einsetzbar
- > Allgemeine Methoden statt protokollspezifischer Speziallösungen, dadurch anpassbar an neue DeFi-Protokolle
- > Nachhaltig verfügbar als Open Source und prototypisch über Iknaio
- > Am Bedarf von Strafverfolgung und Finanzaufsicht ausgerichtet und mit Nutzerinnen und Nutzern validiert
- > Rechtsrahmen (MiCA, DAC8, Transfer of Funds Regulation) mitanalysiert und dadurch anwendungssicher



Anzahl an kriminellen Ereignissen (Counts) im Zusammenhang mit Decentralized Finance und der gemessene Schaden [in USD] in den Jahren 2017-2022.

Experteninterview

Dipl.-Ing. Dr.techn. Stefan Kitzler

Welche wirtschaftlichen und gesellschaftlichen Potenziale sehen Sie für DeFiTrace im internationalen Markt für Krypto-Forensik und Compliance?

Der Bedarf wächst stark, denn immer mehr Länder erhöhen die Regulatorik in diesem Bereich, in Europa etwa mit MiCA und DAC8. Damit steigen die Anforderungen an die Nachvollziehbarkeit von Krypto-Transaktionen erheblich. Strafverfolgung, Finanzaufsicht und regulierte Krypto-Dienstleister brauchen dafür technisch ausgefeilte Werkzeuge, die auf fundierten, wissenschaftlichen Methoden basieren, um Geldflüsse zu verstehen. Genau dort setzt DeFiTrace an. Wirtschaftlich sind Finanzinnovationen ein sehr dynamischer Markt, gesellschaftlich geht es daher darum, mit dieser Dynamik Schritt zu halten und Finanzkriminalität wirksam zu bekämpfen, um das Vertrauen in digitale Finanzmärkte zu stärken und Geschädigte zu schützen.

Für welche Märkte und Anwendungsbereiche ist die Lösung interessant, und wie lässt sie sich skalieren?

Interessant ist sie für all jene, die Zahlungsflüsse analysieren und verstehen müssen, und das vor allem bei großen Fallzahlen. Dazu zählen Strafverfolgungs- und Finanzbehörden, Steuerbehörden und Aufsichtsbehörden sowie Banken und Krypto-Dienstleister. In modernen Finanzsystemen, wie hier im Blockchain- und DeFi-Bereich, lassen sich die anfallenden Transaktionsmengen nicht mehr ausschließlich manuell bewältigen. Analysen brauchen daher eine Form der Automatisierung. Diese Skalierbarkeit muss schon beim Entwickeln der Methoden und Werkzeuge mitgedacht werden. So entstehen technisch nachvollziehbare, skalierbare Lösungen, die sich auf neue DeFi-Protokolle und weitere Blockchains übertragen lassen.

Welche Chancen bietet die in Österreich entwickelte Technologie für den Wirtschafts- und Forschungsstandort?

Österreich kann sich als europäisches Zentrum für Kryp-

© Fotografie Johannes Zimmer



Dipl.-Ing. Dr.techn. Stefan Kitzler
Postdoctoral Researcher,
Complexity Science Hub.

kitzler@csh.ac.at
+43 1 423 010 21 00
https://csh.ac.at

toforensik positionieren und stärkt damit die europäische Unabhängigkeit bei sicherheitsrelevanten Analysetechnologien sowie langfristig den Wirtschaftsstandort. Forschungskonferenzen wie die Advances in Financial Technologies (AFT'24), die im Projektzeitraum von DeFiTrace in Wien stattfand, erhöhen die internationale Sichtbarkeit und ziehen Kooperationen und Talente an. Auszeichnungen wie der Houska-Preis 2024 für die DeFi-Forschung am Complexity Science Hub zeigen, dass wir auf dem richtigen Weg sind. Mit dem wachsenden globalen Markt für Compliance- und Forensiklösungen entsteht zugleich erhebliches Export- und Wertschöpfungspotenzial. ♦

STATEMENT DEVELOPER:

Thomas Niedermayer
Entwickler, Iknaio Cryptoasset
Analytics GmbH



Warum ist DeFiTrace aus Entwicklersicht spannend?

Im Forschungsprojekt DeFiTrace sind Methoden zur Cross-Chain-Verknüpfung und zur automatisierten Pfadanalyse entstanden. Damit konnten wir unsere GraphSense-Plattform gezielt weiterentwickeln und Probleme lösen, an denen herkömmliche Tools scheitern. So unterstützen wir Ermittler:innen direkt in ihrer Arbeit. Forschungsergebnisse so schnell in ein produktives Werkzeug zu bringen, ist für uns technisch wie gesellschaftlich wertvoll.

SICHERHEITS-KLAMMER

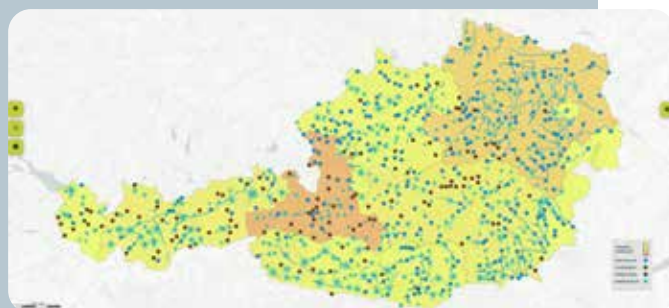
IMPACT LEVEL

5

	1	2	3	4	5	6	7
 SICHERHEIT	☐	☐	☐	☐	☐	☒	☐
 GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☐	☒	☐
 EXPORT POTENTIAL	☐	☐	☐	☐	☒	☐	☐
 WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☒	☐	☐

CESARE

Schaffung einer österreichweiten Schaden- und Ereignisdatenbank



Interaktive Kartenansicht der in CESARE integrierten Schäden und Ereignisse.



Alle Fakten auf einen Blick im Dashboard des Webportals.

STATEMENT DEVELOPER:

Dipl.-Ing. (BA) Steffen Reichel und Matthias Laher, Software-Engineer und GIS-Experte
Spatial Services GmbH

Zahlreiche Institutionen erfassen Schadendaten für ihre eigenen Aufgaben und Anforderungen. Diese unterschiedlichen Datenbestände zu einem nationalen Gesamtbild zusammenzuführen, ist eine anspruchsvolle Herausforderung. CESARE+PLUS adressiert diese Aufgabe mit modernen technischen Lösungen zur Harmonisierung und Aufbereitung der Daten. Für Spatial Services GmbH bietet das Projekt spannende Herausforderungen bei der Entwicklung einer nutzerfreundlichen Anwendung zur Erstellung eines fundierten nationalen Gesamtbildes.

Schaden- und Ereignisdatenbanken sind eine wesentliche Grundlage für ein wirksames Katastrophenrisikomanagement. In Österreich werden Naturgefahren und ihre Auswirkungen von zahlreichen Institutionen erfasst, bislang jedoch nicht in einer österreichweiten und einheitlichen Schaden- und Ereignisdatenbank. Im initialen FFG-KIRAS-Projekt CESARE (Projektende 02/2022) konnten erstmals Schaden- und Ereignisdaten aus unterschiedlichen österreichischen Datenquellen harmonisiert und für die Steiermark sowie Niederösterreich in einem Demonstrator zusammengeführt werden. Seit 2022 wird CESARE von der GeoSphere Austria im Auftrag der ASDR-Plattform betrieben und laufend weiterentwickelt.

Im Folgeprojekt CESARE+PLUS (gefördert durch Innovation AKUT; Projektende 06/2025) erfolgten die Aktualisierung und räumliche Erweiterung des Datenbestands, die Integration zusätzlicher Gefahrentypen sowie die technische Modernisierung von einem ursprünglichen Demonstratorsystem zu einem produktiven, österreichweiten System. Das neue Web-GIS-Portal mit Karten- und Dashboard-Modul ermöglicht die Recherche, Analyse, Visualisierung und den Export harmonisierter Schadensdaten. Damit unterstützt die Plattform Aufgaben im föderalen und nationalen Katastrophenrisikomanagement, Klimawandelanpassung, der nationalen Risikobewertung und das UNDRR-Sendai-Monitoring durch harmonisierte Schadensdaten sowie aussagekräftige Indikatoren und Statistiken für alle Verwaltungsebenen Österreichs.



EXPERTENINTERVIEW

Dr. Stefan Kienberger

Welche wirtschaftlichen Vorteile entstehen für Österreich durch eine nationale Schaden- und Ereignisdatenbank wie CESARE, insbesondere im Hinblick auf effizientere Investitionen in Prävention, Infrastruktur und Risikomanagement?

Eine nationale Schaden- und Ereignisdatenbank wie CESARE bietet vor allem den Vorteil, dass Investitionen in Prävention, Infrastruktur und Risikomanagement deutlich zielgerichteter eingesetzt werden können. Durch die konsolidierte und harmonisierte Datenbasis wird sichtbar, wo tatsächlich die größten Risiken und Schadenspotenziale liegen – und genau dort können Maßnahmen priorisiert umgesetzt werden.

Das führt zu einem effizienteren Mitteleinsatz, vermeidet Fehlallokationen und steigert den Nutzen von Präventionsmaßnahmen. Gleichzeitig können Infrastrukturprojekte besser an reale Gefährdungslagen angepasst werden, was langfristig die Folgekosten durch Schäden reduziert.

Sehen Sie Potenzial, die im Rahmen von CESARE entwickelten Methoden, Standards und Technologien künftig auch international einzusetzen oder als österreichisches Know-how zu exportieren?

CESARE findet bereits heute internationale Beachtung und wurde unter anderem in Berichten der Vereinten Nationen, der Europäischen Kommission (JRC) sowie der Weltbank aufgegriffen. Darüber hinaus erreichen uns zunehmend konkrete Anfragen für einen Erfahrungsaustausch, etwa aus Deutschland, Luxemburg und Schweden. Wir sehen daher ein klares Potenzial, die im Rahmen von CESARE entwickelten Ansätze künftig international zu übertragen. Dies betrifft zum einen den Prozess der Schaffung einer nationalen Schaden- und Ereignisdatenbank sowie die erfolgreiche Einbindung relevanter Akteur:innen. Zum anderen bestehen auch in technischer und inhaltlicher Hinsicht zahlreiche Anknüpfungspunkte für einen Transfer – etwa bei Datenhar-



Dr. Stefan Kienberger
Leiter RiskLab –
Wetter, Klima & Naturgefahren
GeoSphere Austria

stefan.kienberger@geosphere.at
+43 664 614 70 31
www.cesare.at

monisierungsprozessen oder bei der Implementierung des entwickelten WebGIS inklusive zugrunde liegender Datenbankstruktur.

Mit zunehmenden Klimarisiken und steigenden Schadenskosten wächst weltweit der Bedarf an belastbaren Risikodaten. Welche Zukunftsperspektiven sehen Sie für CESARE und welche Rolle könnte das Projekt in den kommenden zehn Jahren für Wirtschaft, Forschung und öffentliche Verwaltung spielen?

Angesichts der erwarteten Zunahme von Extremwetterereignissen wird es immer wichtiger, einen harmonisierten und einheitlichen Überblick über Schadens- und Risikodaten zu schaffen. Nur so kann ein evidenzbasiertes Risikomanagement sowie eine wirksame Klimawandelanpassung unterstützt werden.

Für die Zukunft von CESARE sehen wir großes Potenzial, insbesondere darin, die letzten bestehenden Datenlücken – etwa durch die Einbindung weiterer Akteur:innen – zu schließen. Auf dieser Grundlage eröffnen sich vielfältige Anwendungsmöglichkeiten: von einem kontinuierlichen Monitoring über die Bewertung bis hin zur Wirkungsanalyse gesetzter Maßnahmen. Gleichzeitig ergeben sich künftig weitere Analyseperspektiven, die eine noch tiefere Auswertung von Schadensmustern, Trends und Wirkzusammenhängen ermöglichen. CESARE kann damit als zentrale Entscheidungsgrundlage dienen und einen wichtigen Beitrag für Wirtschaft, Forschung und öffentliche Verwaltung leisten. ♦

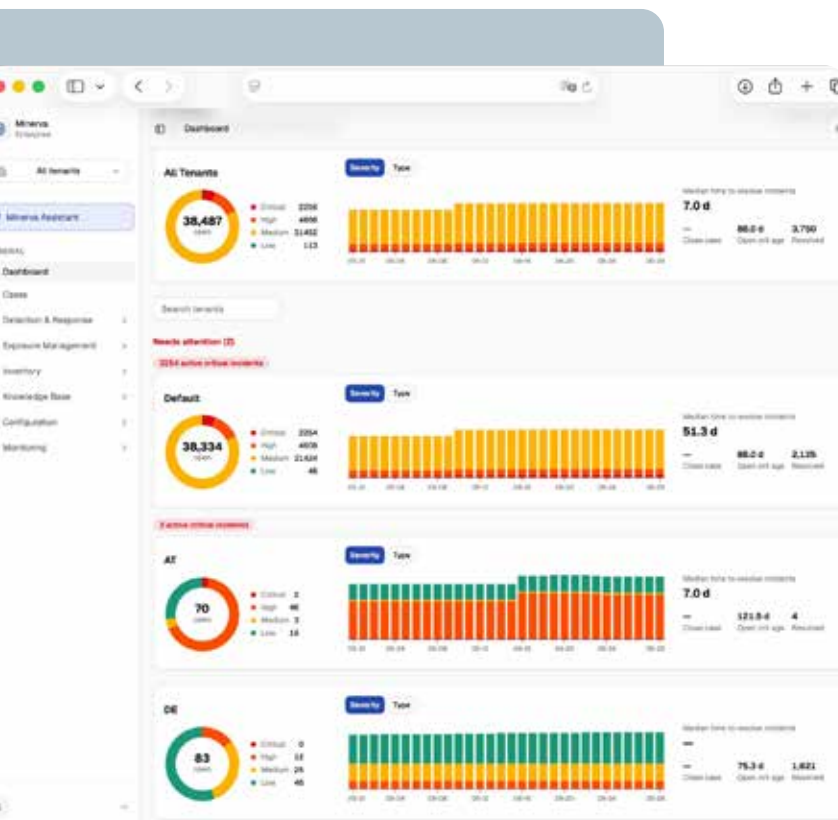
SICHERHEITS- KLAMMER



	1	2	3	4	5	6	7
 SICHERHEIT	☐	☐	☐	☐	☐	☐	☒
 GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☐	☐	☒
 EXPORT POTENTIAL	☐	☐	☐	☐	☒	☐	☐
 WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☐	☐	☒

Minerva

Souveräne KI-Cyberabwehr, die vollständig auf der eigenen Infrastruktur läuft



Cyberangriffe auf Unternehmen, Behörden und kritische Einrichtungen wie Strom-, Wasser- oder Finanzdienste nehmen rasant zu. Angreifer nutzen künstliche Intelligenz. Angriffe, die früher Wochen dauerten, gelingen heute in Minuten. Zur Abwehr braucht es Fachleute, die aus vielen Warnmeldungen die echten Gefahren filtern. Doch sie sind rar. Weltweit fehlen rund 4,8 Millionen Sicherheitsfachkräfte, und 71 % arbeiten schon am Limit, viele nahe am Burnout.

Hier setzt Minerva an. Sie übernimmt die Arbeit erfahrener Sicherheitsfachleute weitgehend selbstständig, wie das erfahrenste Mitglied im Team, das rund um die Uhr Gefahren erkennt, abwehrt und den geschäftlichen Zusammenhang versteht. **Aufgaben, die früher Tage dauerten, erledigt sie in Minuten.**

Minerva läuft vollständig auf der eigenen Infrastruktur. Sensible Daten verlassen diese nie und gelangen nicht in eine fremde Cloud. So behalten Betreiber die Kontrolle, entscheidend dort, wo sicherheitskritische Daten nicht nach außen dürfen. **Kein ausländischer Anbieter kann sie abschalten.** Kunden nutzen Minerva bereits.

VORTEILE:

- > Läuft vollständig in der eigenen Infrastruktur. Keine sensiblen Daten werden in einer fremden Cloud verschickt.
- > Arbeitet rund um die Uhr und ohne Pause, auch dann, wenn Fachkräfte fehlen.
- > Erkennt echte Gefahren in der Flut täglicher Warnmeldungen, schlägt sofort Alarm und leitet Maßnahmen ein.
- > Beschleunigt die Reaktion auf Angriffe und entlastet die Sicherheitsteams.
- > Unabhängig von einem einzelnen ausländischen Anbieter, der den Zugang abschalten könnte.
- > Kann viele Kunden gleichzeitig betreuen. Ideal für IT-Sicherheitsdienstleister.
- > Erfüllt europäische Datenschutz- und Sicherheitsvorgaben.

EXPERTENINTERVIEW

Asif Safdary

Welche wirtschaftlichen Potenziale und Anwendungsbereiche sehen Sie für Minerva?

Das Potenzial liegt in der Verbindung von Eigenständigkeit und Kontrolle über die eigenen Daten. Überall, wo man die Kontrolle über sensible Informationen behalten möchte, etwa bei Strom- und Wasserversorgern, Banken, im Gesundheitswesen, bei Behörden oder der Verteidigung, übernimmt Minerva die Sicherheitsarbeit, ohne etwas nach außen zu geben. Arbeit, die früher Stunden oder Tage gedauert hat, erledigt sie heute in unter fünf Minuten.

Digitale Souveränität ist gerade hochaktuell. Welche Rolle spielt sie für Minerva?

Eine zentrale. Die EU sieht die Abhängigkeit kritischer Infrastruktur von außereuropäischen Anbietern inzwischen als existenzielles Risiko. Wie real das ist, zeigte sich im Juni 2026: Ein großer US-KI-Anbieter musste über Nacht auf behördliche Anordnung seine modernsten KI-Modelle (Fable 5 und Mythos 5) für alle ausländischen Nutzer abschalten. Wer seine Verteidigung an



Asif Safdary
Gründer & CEO,
CyberACI GmbH

asif.safdary@cyberaci.com
www.cyberaci.com

solche fremdgesteuerte Technik bindet, riskiert genau diesen Stillstand. Minerva läuft souverän und ist von außen nicht abschaltbar.

Stichwort „KI gegen KI“. Wie verändert das die Bedrohungslage?

Angreifer setzen immer öfter selbst künstliche Intelligenz ein. Sie suchen nach Schwachstellen rund um die Uhr, nützen sie aus, passen sich an und versuchen es nach jeder Abwehr automatisch erneut. Dieses Tempo ist mit menschlichen Teams allein nicht mehr zu halten. Erst recht bei akutem Fachkräftemangel. Die einzig wirksame Antwort auf angreifende KI ist verteidigende KI. Diese Rolle übernimmt Minerva.

Für welche Märkte ist Minerva interessant, und wie wollen Sie wachsen?

Vor allem für Branchen mit hohen Sicherheits- und Datenschutzanforderungen in Europa und international. Diese Anforderung ist überall dieselbe, daher lässt sich die Lösung gut exportieren. Wachsen wollen wir gemeinsam mit IT-Sicherheitsdienstleistern, die Minerva zu vielen Kunden bringen. Derzeit schließen wir unsere erste größere Finanzierungsrunde ab und erweitern unseren Kundenstamm international, gezielt bei Organisationen, die dieselbe souveräne Haltung teilen und sich nicht von einzelnen Anbietern abhängig machen wollen. ♦

STATEMENT KUNDE:

IT-Leiter eines international tätigen Personaldienstleisters

Zwischen Sicherheit und IT-Betrieb waren wir personell ständig am Limit. Minerva ist zum zusätzlichen Teammitglied geworden, das uns gefehlt hat: Es wertet Warnmeldungen automatisch aus, erkennt Zusammenhänge und verschafft uns wieder Zeit. Dass unsere Daten unter eigener Kontrolle auf unseren eigenen Servern bleiben, ist für uns ein Muss. Unseren externen Dienstleister für die Sicherheitsüberwachung konnten wir schließlich kündigen, weil das Team nun rund um die Uhr einen erfahrenen Sicherheitsanalysten an seiner Seite hat.

SICHERHEITS-KLAMMER



	1	2	3	4	5	6	7
 SICHERHEIT	☐	☐	☐	☐	☐	☐	☒
 GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☐	☒	☐
 EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☒
 WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☐	☒	☐

AIT - AttackBed und Cyber Range

Technologieportfolio für realitätsnahe Cyber-Defence-Test- und Schulungsumgebungen

Cyberangriffe zählen heute zu den zentralen Herausforderungen für Sicherheit und Resilienz. Als Teil hybrider Bedrohungen treffen sie zivile und militärische Infrastrukturen; durch fortschreitende Digitalisierung zunehmend alle militärischen Domänen. Professionelle, gut finanzierte Angreifergruppen wie Advanced Persistent Threats (APT) agieren immer gezielter. Fortschritte im Bereich AI ermöglichen es, Angriffe an spezifische Ziele, Infrastrukturen und Schutzmechanismen anzupassen. Konventionelle und signaturbasierte Sicherheitslösungen stoßen dadurch zunehmend an ihre Grenzen.

Um dieser dynamischen Bedrohungslage zu begegnen, müssen Personal und Cybersicherheitstechnologien unter realistischen Bedingungen getestet, trainiert und weiterentwickelt werden. AIT bietet dafür ein umfassendes Technologieportfolio: AttackMate hilft bei der Analyse der Auswirkungen neuartiger Bedrohungen auf cyber-physische Infrastrukturen, AttackBed ermöglicht Testen von Sicherheitslösungen, und FlowGin, Venjix sowie Learners unterstützen praxisnahes Training, etwa für Cyber Incident Response. Mittels Playbooks und Orchestrierungssoftware können die Technologien automatisiert on-premise, zB der AIT Cyber Range, oder in Public Clouds deployed werden.



VORTEILE:

- > **AttackMate** orchestriert und automatisiert komplexe Angriffsszenarien, die sich wie reale Angriffe in Log- und Netzwerkdaten manifestieren.
- > **AttackBed** simuliert realistische Cyber-Infrastrukturen und bindet Hardware und Digital Twins, z.B. Drohnen, physischer Technologien ein.
- > **FlowGin** und **Venjix** automatisieren Szenarien und nehmen dynamisch Anpassungen basierend auf z.B. Trainingsfortschritt vor.
- > Alle Technologien werden kontinuierlich in internationalen und nationalen Forschungsprojekten in Zusammenarbeit mit behördlichen und industriellen Bedarfsträgern weiterentwickelt.



EXPERTENINTERVIEW

Dr. Markus Wurzenberger

Wie unterscheidet sich AITs AttackBed und Cyber Range Technologieportfolio von anderen?

Alle vorgestellten Technologien sind Open Source und dadurch einsehbar und überprüfbar. Dies gilt auch für generierte Daten die als Open Data veröffentlicht werden. Die Tools werden kontinuierlich in Sicherheits- und Verteidigungsforschungsprojekten weiterentwickelt. Dadurch wird garantiert, dass alle Funktionalitäten am neuesten Stand sind. In Zusammenarbeit mit industriellen und staatlichen Bedarfsträgern werden externe Impulse miteinbezogen, was bei geschlossenen Lösungen nicht möglich wäre. Als non-profit Organisation steht das AIT unter keinem Gewinndruck und kann ein größeres Risiko bei der Entwicklung zukünftiger Technologien eingehen, wodurch ein höheres Innovationspotential besteht.

Welches wirtschaftliche Potential hat das Technologieportfolio und welchen Impact erzeugt es?

AIT nutzt die Technologien, um nationale und internationale Cybersicherheits Schulungen und Trainings durchzuführen. Neben individuell gestalteten Schulungen für Unternehmen, wird seit Jahren das KSÖ Planspiel, eine der größten Cyber Exercises im DACH-Raum, durchgeführt. Darüber hinaus sichern sich Industrieunternehmen, wie z.B. Rheinmetall, Nutzungsrechte und Ausbildungszeiten, um das Produktportfolio zum Testen eigener Technologien und zur Schulung von Personal einzusetzen. AITs Technologien werden in allen laufenden Cyber-Projekten des European Defence Fund (EDF) eingesetzt. Besonderer Fokus liegt auf der Umsetzung realistischer Demos für Europäische Militärs am AttackBed und mit dem AttackMate. Zentrales Augenmerk liegt auf der Generierung von realistischen gelabelten Datensets zur Entwicklung neuer Verteidigungstechnologien im Cyberbereich, wobei besonders im militärischen Umfeld die Einbindung Cyber-physischer System (z.B. Drohnen) essenziell ist.



Dr. Markus Wurzenberger
AIT Austrian Institute of Technology GmbH

markus.wurzenberger@ait.ac.at
+43 664 815 79 37

Welche Entwicklungen sind nötig, um mit der sich rasch entwickelnden Cyberbedrohungslage Schritt zu halten?

Da Cyberangriffe zunehmend ausgeklügelter werden und Netzwerke und Systeme sich immer rascher verändern, müssen auch Test- und Schulungssysteme mit neuen Entwicklungen Schritt halten. Um dieser Dynamik gerecht zu werden, wird ein hoher Grad an Automatisierung benötigt. AI und im Speziellen Agentic AI bieten hier neue Möglichkeiten, um rasch auf geänderte Anforderungen zu reagieren. ♦

STATEMENT DEVELOPER:

Klaus Mayer, MSc
AIT Austrian Institute of Technology GmbH



Warum ist AITs Testbed und CR Portfolio aus Expertensicht spannend?

Im Gegensatz zu anderen ermöglichen AITs Technologien eine individuelle Anpassung und dynamischer Erweiterung von Infrastrukturen und Szenarien. Weiters wird vor allem bei der Umsetzung von Angriffssimulationen starker Fokus auf Realismus gelegt, was essenziell ist, um Erkenntnisse auf die reale Welt umlegen zu können. Der Forschungs- und Open Source-basierte Ansatz fördert technische Aktualität und Sicherheit.

SICHERHEITS-KLAMMER

IMPACT LEVEL

6

	1	2	3	4	5	6	7
SICHERHEIT	☐	☐	☐	☐	☐	☒	☐
GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☐	☒	☐
EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☒
WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☒	☐	☐

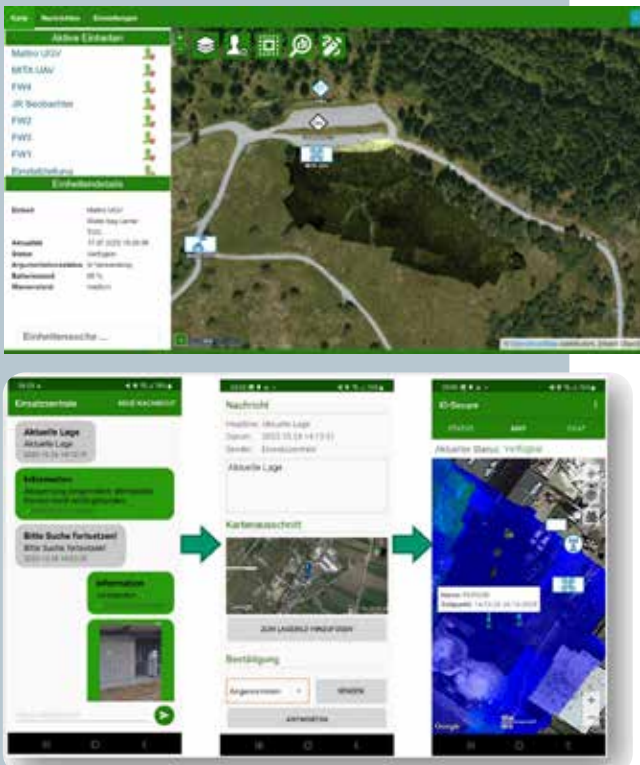
KI-SecAssist

KI-gestützte Einsatzunterstützung in Krisensituationen



© JOANNEUM RESEARCH

Im Rahmen des KIRAS-Projekts KI-SecAssist entwickelten Forscher*innen einen Demonstrator zur KI-basierten Unterstützung von Einsatzkräften in Krisen- und Katastrophensituationen. Ziel war es, unbemannte Luftfahrzeuge (UAVs) und Bodenfahrzeuge (UGVs) mit KI-gestützter Sensorik und einem kooperativen Aufgabenmanagement zu vernetzen, um Einsatzleitungen in Echtzeit mit entscheidungsrelevanten Informationen zu versorgen. Das System ermöglicht die autonome Erfassung und Analyse von Sensordaten sowie die Bereitstellung eines aktuellen Lagebildes. Im Projekt wurden Verfahren zur Sensorfusion, semantischen Segmentierung sowie zur Detektion von Personen, Fahrzeugen und Glutnestern entwickelt und in ein Gesamtsystem integriert. Ergänzt wurden diese durch Funktionen für ein kooperatives Aufgabenmanagement, die Kommunikation zwischen den Systemen, multimodale Einsatzunterstützung sowie Schnittstellen zu externen Anwendungen. Die entwickelten Technologien wurden in zwei realitätsnahen Szenarien demonstriert: einem Industrieunfall auf dem Betriebsgelände der Firma Messer mit einem simulierten Gasaustritt sowie einem Waldbrand-szenario im Rahmen der Übung AART 2023 auf der Seetaler Alpe. Dabei kamen automatisierte Befliegungen, KI-gestützte Objekterkennung, mobile Lagebilder sowie die koordinierte Zusammenarbeit von UAVs, UGVs und Einsatzkräften zum Einsatz. In die Demonstrationen waren unter anderem die Berufsfeuerwehr Graz, die Freiwillige Feuerwehr Gumpoldskirchen sowie weitere Bedarfsträger des Projekts eingebunden. Das Projekt zeigte das Potenzial KI-basierter Assistenzsysteme, Einsatzkräfte zu entlasten und die Entscheidungsfindung in komplexen Lagen zu unterstützen.



Ein Echtzeit-Lagebild liefert einen wesentlichen Beitrag dazu, Einsatzkräfte bei komplexen Entscheidungen datenbasiert zu unterstützen.



© TWINS

EXPERTENINTERVIEW

DI Dr. Markus Bergen, BSc

Welches Potenzial hat KI-SecAssist über ein Forschungsprojekt hinaus?

Sinnvolle Entscheidungsunterstützung passiert jetzt schon durch die angesprochenen Technologien, oft aber noch als Einzeltools zur Erweiterung bestehender Fähigkeiten. Der Einsatz von Drohnen ist bereits tägliche Praxis, die systematische Zusammenführung der erfassten Daten zu einem digitalen Lagebild jedoch deutlich seltener. Aktuell entsteht dieses Lagebild auf Basis der Erfahrung der Einsatzleitung und im Zusammenspiel mit dem Team. Zukünftig wird es entscheidend sein, dieses Expertenwissen bestmöglich mit den KI-gestützten Technologien zu verknüpfen. Neue Technologien sollen vor allem niederschwellig unterstützen und keine zusätzlichen Ressourcen binden. Hier besteht noch Forschungsbedarf: auf technischer Ebene – etwa bei der Automatisierung und Integration verschiedener Systeme – und hinsichtlich Prozessoptimierung im Zusammenspiel von Menschen und KI.

Wie gelingt der Transfer in die Praxis?

2026 hat sich unter anderem aus diesem Projekt heraus ein Spin-off der JOANNEUM RESEARCH entwickelt. Ein internationaler Investor hat das Unternehmen lagebild.one ermöglicht, das die Technologien, die auch bei KI-SecAssist maßgeblich sind, weiterentwickeln werden. Damit wird ein TRL von 7-8 möglich.

Für welche Anwendungsbereiche beziehungsweise Bedarfsträger sind die Projektergebnisse relevant?

Ganz klar für all jene Bereiche, in denen komplexe, problematische oder kritische Situationen von unterschiedlichen Akteur:innen gelöst werden müssen.



© JOANNEUM RESEARCH/Bergmann

DI Dr. Markus Bergen, BSc
Koordinator Geschäftsfeld
Sicherheit und Verteidigung

Markus.Bergen@joanneum.at

Markus Bergen ist Koordinator für das Geschäftsfeld Sicherheit und Verteidigung und Spezialist für photogrammetrische Bildverarbeitung, Geoinformationsdienste und Multi-Sensor-Systeme und seit Oktober 2023 bei JOANNEUM RESEARCH DIGITAL in der Forschungsgruppe Fernerkundung und Geoinformation. Aktuell beschäftigt er sich vorrangig im Bereich Sicherheit und Verteidigung mit der Bereitstellung umfassender Lagebildinformationen durch den Einsatz mobiler Plattformen (UxVs), tragbarer Sensorik, Geodatenanalysen und Sensorfusion.

Das sind die Polizei, das Militär, der Grenzschutz oder die Küstenwache, der Katastrophenschutz oder die Feuerwehr, das THW (Technisches Hilfswerk), Rettungsdienste, Land und Forstwirtschaft oder Ausbildungseinrichtungen. Es geht immer darum, Menschen bei komplexen Entscheidungen datenbasiert zu unterstützen und damit auch die Sicherheit für Beteiligte zu erhöhen. ♦

SICHERHEITS- KLAMMER

IMPACT LEVEL
3

	1	2	3	4	5	6	7
SICHERHEIT	☐	☐	☐	☒	☐	☐	☐
GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☒	☐	☐
EXPORT POTENTIAL	☐	☐	☐	☐	☐	☒	☐
WIRTSCHAFTLICHES POTENTIAL	☐	☐	☐	☐	☐	☒	☐

DesinFact

Früherkennung möglicher Desinformationstrends durch verantwortungsvolle datenbasierte Analyseansätze



DesInfact Plugin

☒ Ich habe gelesen und stimme der EULA zu.

☒ Ich erkläre mich damit einverstanden, dass die von mir aufgerufenen Websites zur automatischen Überprüfung an eine künstliche Intelligenz übermittelt wird.

Activate

Bitte beachten Sie: Wenn Sie dem EULA (Punkt 1) oder der automatischen Prüfung (Punkt 2) nicht zustimmen, erhalten Sie keine Risikobewertung für noch unbekannte Websites und tragen nicht zur Verbesserung des Plugins bei.

Desinformation kann im Rahmen hybrider Bedrohungslagen kritische Infrastrukturen sowie demokratische Prozesse beeinträchtigen. Eine frühzeitige Erkennung möglicher Desinformationstrends kann Institutionen dabei unterstützen, Entwicklungen besser einzuordnen und geeignete Maßnahmen vorzubereiten. Das KIRAS-Projekt DesinFact untersuchte daher wissenschaftliche Ansätze zur verantwortungsvollen Unterstützung der Früherkennung von Desinformation. Im Mittelpunkt standen Methoden zur Analyse von Kommunikations- und Netzwerkstrukturen sowie inhaltsbezogenen Merkmalen, um Hinweise auf koordinierte Verbreitungsmuster zu identifizieren. Dabei wurde bewusst auf automatisierte Wahrheits- oder Falschheitsbewertungen verzichtet. Stattdessen erforschte das Projekt nachvollziehbare Analyseverfahren, deren Ergebnisse als Entscheidungshilfe für Expert:innen dienen können. Ein weiterer Schwerpunkt lag auf der transparenten Darstellung von Analyseergebnissen sowie auf rechtlichen, ethischen und datenschutzrechtlichen Fragestellungen. Die Projektergebnisse zeigen, dass technische Unterstützung einen Beitrag zur strukturierten Analyse leisten kann, sofern hohe Qualitätsstandards eingehalten und menschliche Bewertung nicht ersetzt wird.

VORTEILE:

- > Früherkennung möglicher Desinformationstrends
- > Analyse von Kommunikations- und Netzwerkstrukturen
- > Kombination struktur- und inhaltsbezogener Analyseansätze
- > Erklärbare und nachvollziehbare Analyseverfahren
- > Unterstützung menschlicher Bewertung statt automatisierter Wahrheitsentscheidungen
- > Berücksichtigung rechtlicher, ethischer und datenschutzrechtlicher Anforderungen
- > Untersuchung prototypischer Ansätze für öffentliche Analysewerkzeuge
- > Erforschung transparenter Ergebnisdarstellungen zur Unterstützung von Entscheidungsprozessen

EXPERTENINTERVIEW

Dr. Mina Schütz, B.Sc., M.Sc.

Welche Anwendungsbereiche sehen Sie für die im Projekt DesinFact entwickelten Ansätze?

Ein Schwerpunkt von DesinFact lag auf der Frage, wie technische Analyseverfahren Endanwender:innen bei der Einordnung von Online-Inhalten unterstützen könnten. Im Projekt wurden prototypische Ansätze untersucht, die Nutzer:innen strukturierte Hinweise liefern, ohne automatisierte Wahrheits- oder Falschheitsentscheidungen zu treffen. Dabei standen insbesondere die verständliche Darstellung der Ergebnisse, Transparenz sowie Fragen der Anonymität, Qualitätssicherung und Missbrauchsvermeidung im Mittelpunkt. Die Projektergebnisse bilden eine Grundlage für die weitere Erforschung solcher unterstützenden Ansätze.

Wo sehen Sie das größte Potenzial der Projektergebnisse?

Das größte Potenzial liegt aus unserer Sicht in der Verbindung unterschiedlicher Analyseperspektiven. Im Projekt konnte gezeigt werden, dass die Kombination von Netzwerkstrukturen, Kommunikationsmustern und inhaltsbezogenen Analysen ein umfassenderes Bild möglicher Desinformationstrends liefern kann als isolierte Einzelverfahren. Gleichzeitig hat DesinFact verdeutlicht, dass Transparenz, Erklärbarkeit und Vertrauenswürdigkeit wesentliche Voraussetzungen für den verantwortungsvollen Einsatz solcher Technologien sind. Diese Erkenntnisse bilden eine wichtige Grundlage für die weitere Forschung und Entwicklung in diesem Bereich.

Welche Perspektiven eröffnen die Projektergebnisse für Forschung und Praxis?

DesinFact hat gezeigt, dass eine verantwortungsvolle technische Unterstützung bei der Analyse von Informationsräumen grundsätzlich möglich ist. Gleich-



Dr. Mina Schütz, B.Sc., M.Sc.
Data Science & Artificial Intelligence
Center for Digital Safety & Security
AIT Austrian Institute of
Technology GmbH

Mina.schuetz@ait.ac.at
www.ait.ac.at

zeitig wurden offene Forschungsfragen identifiziert, etwa zur mehrsprachigen Analyse, zur langfristigen Beobachtung narrativer Entwicklungen oder zur adressatengerechten Darstellung komplexer Analyseergebnisse. Die Projektergebnisse bilden damit eine Grundlage für weiterführende Forschung und können dazu beitragen, zukünftige Analysewerkzeuge transparenter, robuster und vertrauenswürdiger zu gestalten. Langfristig könnten solche Systeme insbesondere Fachanwender:innen wie Journalist:innen, Fact-Checker:innen oder Behörden bei ihrer täglichen Arbeit unterstützen. ♦

STATEMENT SENIOR SCIENTIST:

Dr. Alexander Schindler
alexander.schindler@ait.ac.at



Desinformation ist ein komplexes gesellschaftliches Phänomen, das sich nicht auf einfache technische Lösungen reduzieren lässt. DesinFact hat gezeigt, dass vertrauenswürdige Unterstützung nur dann möglich ist, wenn technische Leistungsfähigkeit, Transparenz, Erklärbarkeit sowie rechtliche und ethische Anforderungen gemeinsam gedacht werden. Unser Ziel war daher nicht die Automatisierung von Bewertungen, sondern die Erforschung nachvollziehbarer Methoden, die Expert:innen bei der Analyse unterstützen können.

SICHERHEITS- KLAMMER

IMPACT LEVEL



	1	2	3	4	5	6	7
SICHERHEIT	☐	☐	☒	☐	☐	☐	☐
GESELLSCHAFTLICHER NUTZEN	☐	☐	☐	☐	☐	☐	☒
EXPORT POTENTIAL	☐	☐	☐	☐	☒	☐	☐
WIRTSCHAFTLICHES POTENTIAL	☐	☐	☒	☐	☐	☐	☐

Die Österreichische Sicherheitsklammer



FÜR DIE ENGLISCHE VERSION
BITTE WENDEN 

PLEASE TURN
FOR THE ENGLISH VERSION