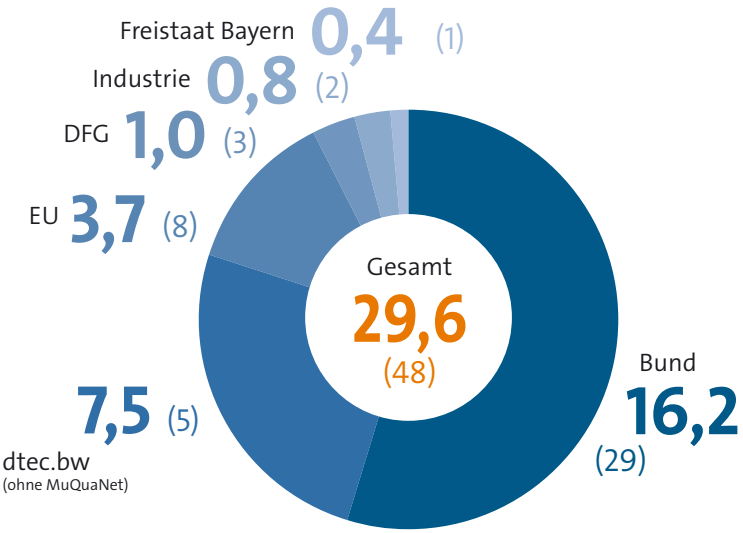

der Bundeswehr
Universität München
CODE
JAHRESBERICHT
2025
CODE
FI
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Projektförderung

2025 wurden insgesamt 48 drittmittelfinanzierte Projekte am FI CODE bearbeitet oder eingeworben. dtec.bw-Projekte erhalten Mittel aus dem Etat des Geschäftsbereichs BMVg.

Drittmittel*



* Angaben in Millionen Euro, Anzahl der Projekte in Klammern.

dtec.bw-Projekt**

MuQuaNet – Das Quanten-Internet im Großraum München

MuQuaNet
The Munich Quantum Network

Beteiligte Professuren

Prof. Dr. Wolfgang Hommel
Hon.-Prof. Dr. Udo Helmbrecht
Prof. Dr. Michaela Geierhos
Prof. Dr. Arno Wacker

** Unter Beteiligung des FI CODE mit Projektstart im Jahr 2020, nicht in der Drittmittel-Übersicht (links) enthalten.

Internationalität

Das FI CODE unterhält ein internationales Netzwerk.

Mitarbeitende***

Die Mitarbeitenden des FI CODE stammten im Jahr 2025 aus 19 Ländern.

Kooperationspartner***

Im Jahr 2025 arbeitete das FI CODE mit 79 Partnern in 27 Ländern zusammen.

Legende

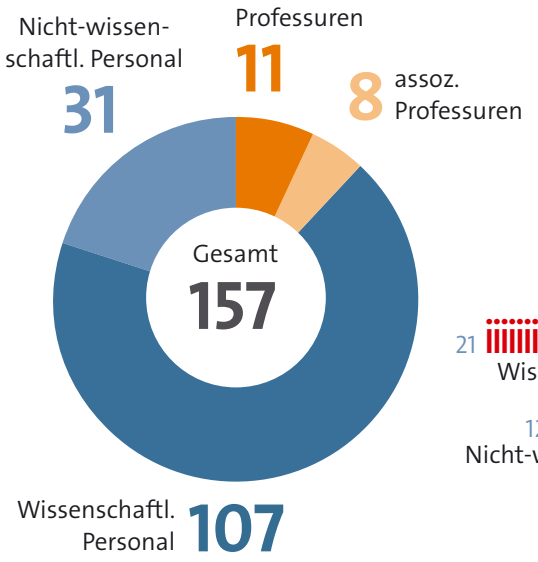
- Standort FI CODE
- 1 — Anzahl von CODE-Mitarbeitenden aus den Herkunftsländern
- 1 — Anzahl internationaler Kooperationspartner im betreffenden Land
- Länder mit Kooperationspartnern und Mitarbeitenden

*** Weitere Informationen zu Kontakten und Kooperationspartnern finden Sie ab S. 76.

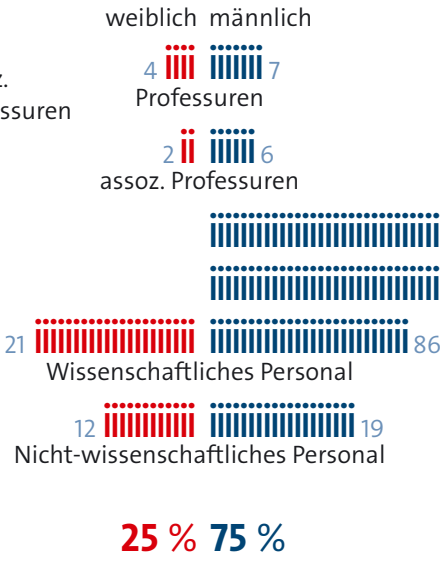
Personalstruktur

Das FI CODE hatte 2025 insgesamt 157 Mitarbeitende. Der Frauenanteil betrug 25 %.

Mitarbeitende



Geschlechteranteil



25 % **75 %**

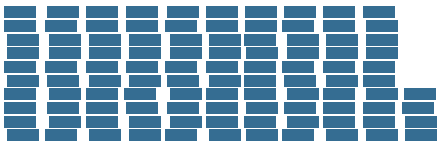
Forschungsarbeit

Übersicht der Promotionen und Publikationen am FI CODE 2025

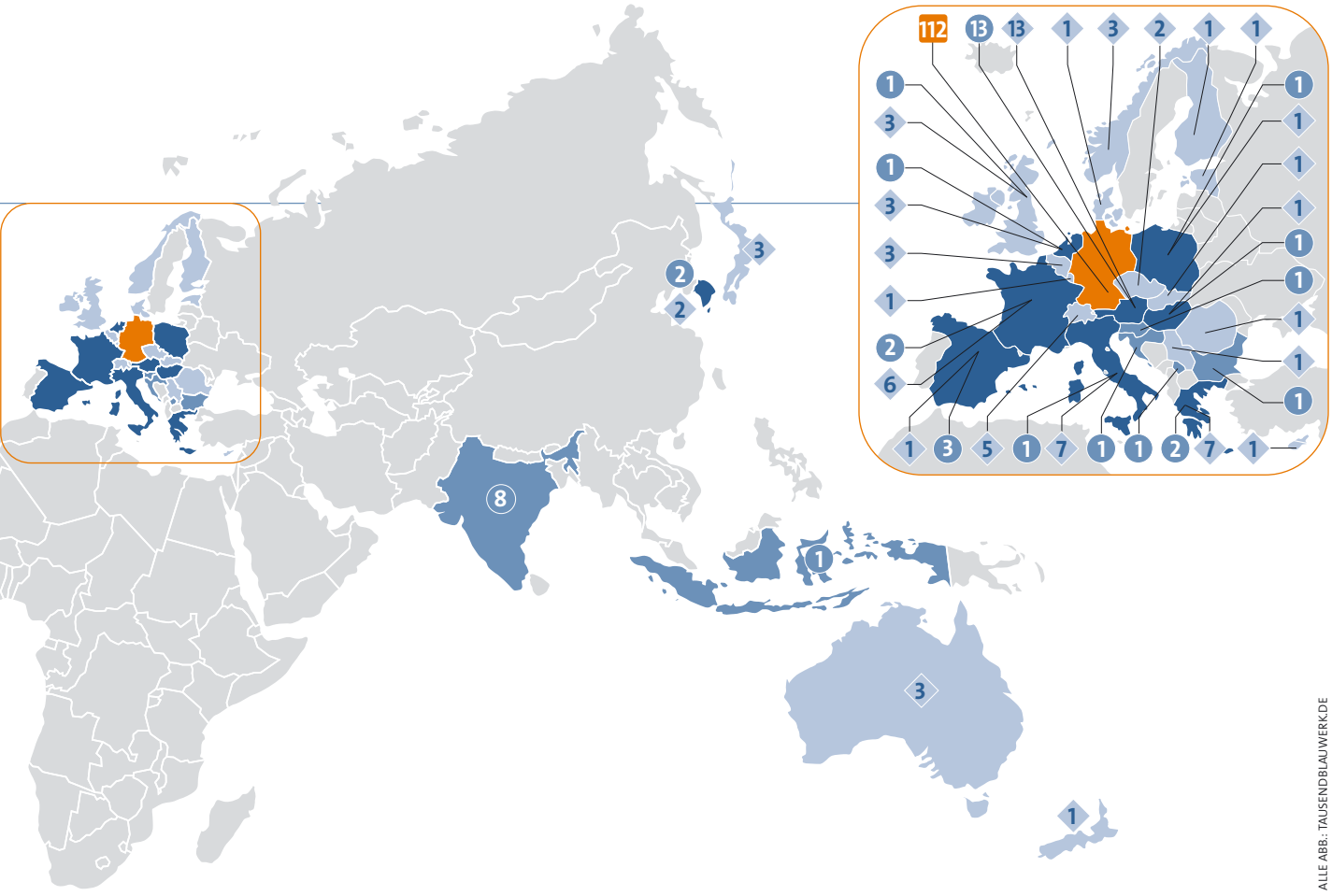
Promotionen

5

Publikationen



104



ALLE ABB.: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
JAHRESBERICHT
2025

FI CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Vorwort der Präsidentin

Die fortschreitende Digitalisierung und die zunehmende Vernetzung kritischer Systeme stellen Gesellschaft, Wirtschaft und staatliche Akteure vor wachsende Herausforderungen. Cybersicherheit ist dabei zu einem zentralen Faktor für Resilienz, Handlungsfähigkeit und technologische Souveränität geworden. Angesichts der stetig zunehmenden Cyberangriffe auf kritische Infrastrukturen, Unternehmen und Privatpersonen ist es daher unerlässlich, die Forschung in diesem Bereich gezielt und nachhaltig voranzutreiben.

Das Forschungsinstitut CODE leistet hierzu auf nationaler und internationaler Ebene einen wesentlichen Beitrag. Damit stärkt es zugleich nachhaltig das Profil der Universität der Bundeswehr München als eine der führenden Institutionen für Sicherheit und Resilienz in Technik und Gesellschaft.

Das Jahr 2025 war für CODE von der Weiterentwicklung zentraler Kooperationen sowie von erfolgreichen Forschungsaktivitäten geprägt. Mit der Unterzeichnung eines Memorandum of Understanding wurde die langjährige Zusammenarbeit zwischen der Universität der Bundeswehr München und Airbus weiter gefestigt. Ziel der Partnerschaft ist es, gemeinsame Forschungsprojekte, insbesondere in den Bereichen Sicherheit, Verteidigung, Luft- und Raumfahrt sowie Cybersicherheit auszubauen.

Auch in der angewandten Forschung konnte CODE wichtige Fortschritte erzielen. So wurde mit dem Projekt *MERLIN* in Kärnten ein neuartiges experimentelles Blackout-Kommunikationssystem vorgestellt, das eine regionale Kommunikation auch bei Ausfällen bestehender Infrastrukturen ermöglicht. Durch den Start des EU-geförderten Projekts *PiQASO* baute CODE zudem die internationale Zusammenarbeit weiter aus. Gemeinsam mit 24 Partnern arbeitet das Institut an kryptographischen Grundlagen für eine quantensichere Kommunikation in Europa.

Neben der Forschung bildeten Nachwuchsförderung und das Engagement für Vielfalt, Gleichstellung und Chancengerechtigkeit einen weiteren Schwerpunkt. Beim *„Girls' Day 2025"* erhielten 30 Schülerinnen Einblicke in Studienmöglichkeiten und aktuelle Themen der Cybersicherheit. Darüber hinaus fand ein mehrtägiger Ferienworkshop für Mädchen statt, der Grundlagen von Elektronik, Sensorik und Programmierung praxisnah vermittelte. Für ihr langjähriges Engagement wurden Dr. Siegfried Brunner und Ulrike Nussel mit dem Diversity-Preis der UniBw München ausgezeichnet.

Ein Höhepunkt des Jahres war die *CODE-Jahrestagung 2025* mit über 500 Teilnehmenden aus Wissenschaft, Bundeswehr, Behörden und Wirtschaft, die den fachlichen Austausch zur Cyber-Resilienz weiter stärkte.

Das Forschungsinstitut CODE trägt mit seinen Projekten dazu bei, Deutschland und die Welt sicherer zu machen. Es entwickelt innovative Lösungen für die Herausforderungen von morgen und stärkt unsere digitale Resilienz. Ich gratuliere dem gesamten Institut zu einem abermals erfolgreichen Jahr! Freuen Sie sich auf interessante Einblicke in die Welt der Cybersicherheit!

Mit den besten Grüßen

Prof. Dr. mont. Dr.-Ing. habil. Eva-Maria Kern, MBA
Präsidentin Universität der Bundeswehr München

Marcus Knüpfer, Michaela Geierhos und Wolfgang Hommel

Liebe Leserinnen und Leser,

mit seiner technisch tiefgehenden Expertise und zahlreichen gelungenen Beispielen dafür, wie universitäre Forschung erfolgreich in die Praxis überführt werden kann, war das Forschungsinstitut CODE auch 2025 wieder ein verlässlicher Partner für die Bundeswehr, Behörden und die Industrie. Wir haben uns in diesem Jahr besonders über die tatkräftige Verstärkung durch neue Forschungsgruppen gefreut: Neben der Berufung von Prof. Dr. Michael Hutter auf die CODE-Professur für Embedded System Security in der Fakultät für Informatik wirken seit dem Berichtsjahr Prof. Dr.-Ing. Carmen Mas Machuca (Professur für Kommunikationsnetze, Fakultät EIT), Prof. Dr.-Ing. Vladislav Nenchev (Professur für Embedded Systems, Fakultät ETTI) und Prof. Dr. Christoph Peters (Professur für Wirtschaftsinformatik, insb. Digital Process Management, Fakultät WOW) mit ihren Teams als assoziierte Mitglieder am FI CODE mit und tragen zur weiteren Verbreiterung unseres Kompetenzspektrums bei.

Die Relevanz der diesjährigen Schwerpunktthemen, wie beispielsweise Künstliche Intelligenz, zeigt sich nicht nur in zahlreichen anwendungsorientierten Forschungsprojekten, in die der vorliegende Jahresbericht einen Einblick gewährt, sondern auch in einer Reihe öffentlichkeitswirksamer Veranstaltungen. So sorgte beispielsweise ein Münchner KI-Themenmonat für volle Hörsäle und auch eine Kinderuni-Vorlesung zum Thema KI begeisterte zahlreiche Schülerinnen und Schüler.

Selbstverständlich hält die thematische Weiterentwicklung auch Einzug in die Lehre. Die neue Vertiefungsrichtung „Künstliche Intelligenz" im Masterstudiengang Informatik bündelt über 50 Lehrveranstaltungen in neuen Modulen. Diese lassen Wahlmöglichkeiten für eine technische Spezialisierung oder eine Anwendungsorientierung zu und werden zu einem großen Teil von Kolleginnen und Kollegen aus dem FI CODE angeboten.

Durch die fakultätsübergreifende Bündelung der KI-Expertise der Universität der Bundeswehr München im Kompetenzzentrum Künstliche Intelligenz (KompZ KI) entsteht ein starker, technischer und methodenorientierter Nukleus mit vielfältigen Anwendungsdomänen. Diesen entwickeln wir gemeinsam mit unseren Partnern.

Zu unseren Partnern zählen auch Vertreter anderer Fachbereiche. So durften wir Host mehrerer Cyber-Übungen wie der Defence Cyber Marvel (DCM4) oder der Cyber Phoenix für die Cyber-Reserve der Bundeswehr sein. Das OSINT-Forum hat sich im Jahr 2025 erfolgreich als Format etabliert, das Industrie-Experten und OSINT-Spezialisten der Bundeswehr und Sicherheitsbehörden eine Plattform für den Austausch bietet.

Wir wünschen Ihnen beim Lesen unseres Jahresberichts 2025 spannende Unterhaltung und freuen uns auf weitere gemeinsame Aktivitäten in der Zukunft!

Prof. Dr. Wolfgang Hommel

Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Leitung des Forschungsinstituts CODE

ABB.: UNIBW M; A. WAGENER FOTOGRAFIE

Inhalt

ABB.: ADOBE STOCK / ANDYAZIZ6

Highlights
Aus dem Institut

Forschung
Porträts und Projekte

Weitere Forschungsgruppen und Projekte

Kooperationen
Deutschland und die Welt

Nachwuchsförderung
Chancen und Angebote

Addendum
Publikationen und Aktivitäten

Organisation

Rubriken

UNSER BILD

ABB.: ADOBE STOCK / GREENBUTTERFLY

Das Forschungsinstitut CODE ist eine zentrale wissenschaftliche Einrichtung der Universität der Bundeswehr München. Wir setzen unsere Expertise zum Mehrwert der Gesellschaft und der Bundeswehr ein und tragen durch Innovationen im Bereich Cyber/IT dazu bei, Deutschland ein Stück sicherer zu machen.

Drei Säulen stehen dabei im Fokus unseres Handelns:

- **Forschung und Technologie-Entwicklung**
- **Wissenstransfer sowie Beratung von Entscheidungsträgern**
- **Aus- und Weiterbildung**

Wir betreiben sowohl Grundlagen- als auch anwendungsnahe Forschung und Technologie-Entwicklung in den Themenfeldern Cyber Defence, Smart Data und Quantum Technology. Unsere Arbeit fokussiert sich dabei auf den konkreten und perspektivischen Nutzen für die Gesellschaft und die Bundeswehr. Durch unsere engen Verbindungen mit der Teilstreitkraft CIR (Cyber- und Informationsraum) der Bundeswehr sind wir in einer einzigartigen Position, durch Forschung in einer sicheren Umgebung Lösungen für die aktuellen und zukünftigen Herausforderungen in der Domäne CIR zu erarbeiten.

Unser Ziel ist es, technische Innovationen und Konzepte zum Schutz von Daten, Software und Systemen ganzheitlich und interdisziplinär zu erforschen. Wir legen besonderen Wert darauf, anwendungsnahe Technologien zu entwickeln und die gesellschaftliche Akzeptanz für sichere Technologien zu fördern. Dafür arbeiten wir eng mit der Bundeswehr, Behörden, Forschungseinrichtungen und der Wirtschaft zusammen, damit unsere Partner neue Forschungserkenntnisse und Technologien wertschöpfend in die Praxis transferieren können.

Wir sind offen für den wissenschaftlichen Diskurs und verfolgen langfristige Kooperationen. Mit den breit gefächerten Kompetenzen unserer Professuren und Forschungsgruppen stehen wir Entscheidungsträgern aus Bundeswehr und Politik beratend zur Seite und fördern den Wissenstransfer. Unser wissenschaftlicher Beirat unterstützt das FI CODE mit seiner fachlichen Expertise aktiv bei der strategischen Weiterentwicklung.

Für die Aus- und Weiterbildung bieten wir optimale Rahmenbedingungen. Unsere IT-Infrastruktur erlaubt Forschung und Ausbildung auf höchstem Niveau. Wir bereiten in der Lehre Studierende an der Universität der Bundeswehr München auf die Herausforderungen ihres Berufslebens vor und bilden Angehörige der Bundeswehr und Cyber-Reserve in unserer modernen Cyber Range praktisch weiter. Der direkte Zugang zu Quantencomputern ermöglicht uns bereits heute, innovative Lösungen für die Herausforderungen von morgen zu finden.

Wir stehen zu unserer Verantwortung und Vorbildfunktion, gemeinsam mit unseren Partnern und vor allem der Bundeswehr für den Schutz der freiheitlichen demokratischen Gesellschaft einzutreten. Wir arbeiten täglich daran, einen wesentlichen Beitrag zum Schutz vor den Gefahren im Cyber- und Informationsraum zu leisten und sind bereit, uns daran messen zu lassen.

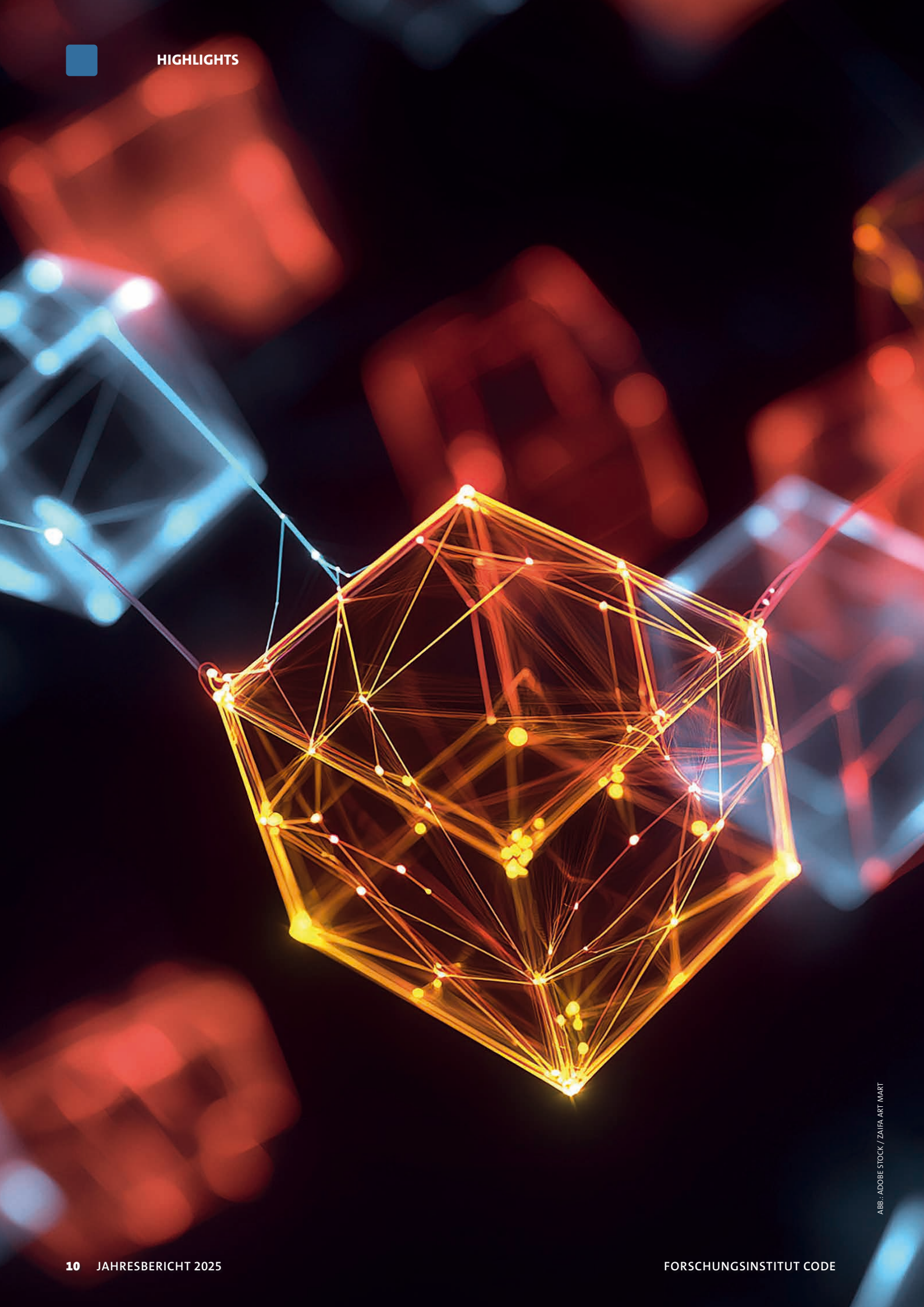


ABB.: ADOBE STOCK / ZAIFA ART MART

Highlights

Aus dem Institut

CODE-Jahrestagung 2025

Die Cyber-Resilienz von morgen – proaktiv statt reaktiv

Auch 2025 kamen bei der Jahrestagung des Forschungsinstituts Cyber Defence und Smart Data (CODE) wieder weit über 500 Expertinnen und Experten aus Wissenschaft, Bundeswehr, Behörden und Wirtschaft zusammen, um sich über aktuelle Fragestellungen der Cyber-Resilienz auszutauschen und gemeinsam einen Blick in die Zukunft der Cybersicherheit zu werfen.

VON BENJAMIN BELLGRAU

BEIDE ABB.: FI CODE / ANGELIKA WAGENER FOTOGRAFIE

NACH DER BEGRÜSSUNG durch den Vizepräsidenten der Universität der Bundeswehr München (UniBw M), Prof. Dr. Karl-Heinz Renner, gab der Leitende Direktor von CODE, Prof. Dr. Wolfgang Hommel, den Teilnehmenden der Jahrestagung einen Einblick in die aktuellen Entwicklungen am Forschungsinstitut. Neben drei neuen Fachgruppen konnte man sich bei CODE in den zurückliegenden zwölf Monaten über neue Forschungsprojekte, insbesondere im Bereich der Quantentechnologien, freuen. Auch die Entwicklungen im Bereich der Künstlichen Intelligenz hob er hervor. So wird ab Januar 2026 eine neue KI-Vertiefungsrichtung im Masterstudiengang Informatik an der UniBw M angeboten. Darüber hinaus ist an der Universität auch die Einrichtung eines interdisziplinären KI-Kompetenzzentrums geplant.

Keynote Speaker aus Bundeswehr, Behörden und Industrie

In einer Zeit, in der Cyberbedrohungen immer komplexer und raffinierter werden, ist es unerlässlich, nicht nur auf Angriffe zu reagieren, sondern ihnen proaktiv entgegenzuwirken. Cyber-Resilienz bedeutet, Systeme so zu gestalten, dass sie Angriffen standhalten und sich schnell von ihnen erholen können. Dies erfordert ein Zusammenspiel von Technologie, Prozessen und Menschen. Cyberangriffe, Datenlecks und Systemausfälle sind keine Ausnahmeerscheinungen mehr, sondern Realität. Diese Realität verlangt nach einem Paradigmenwechsel: weg vom reinen Krisenmanagement, hin zu strategischer Vorsorge. Hierfür ist eine technologische Zeitenwende erforderlich.

Innovative Technologien müssen schnell identifiziert und in die Anwendung gebracht werden, um eine kriegstüchtige und zukunftsorientierte Bundeswehr sicherzustellen. In seiner Keynote betonte Generalleutnant Michael Vetter, Abteilungsleiter Cyber-/Informationstechnologie im Bundesministerium der Verteidigung (BMVg), dass hierfür auch mehr Risikobereitschaft nötig sei.

Auch die Wissenschaft ist von der Zeitenwende zunehmend betroffen. In einer von globalen Spannungen geprägten Welt rückt sie als hochwertiges und attraktives Ziel immer mehr in den Fokus von Angreifern. Doch wie kann der Spagat zwischen Wissenschaftsfreiheit und Sicherheit gelingen? Barbara Kluge, Ministerialdirigentin im Bundesministerium des Innern, betonte in diesem Zusammenhang die Rolle des Staates, der „Verantwortung für den Schutz der Wissenschaft auch im Cyberraum trägt“, und rief zu raschem gemeinsamen Handeln auf.

Generalleutnant Michael Vetter während seiner Keynote.

Anschließend sprach Generalmajor Jürgen Setzer in seiner Keynote zum Thema „(Cyber-) Resilienz heute und morgen“ über die Bedeutung strategischer Voraussicht und führte aus: „Krieg ist nicht nur ein Innovationswettkampf, sondern auch ein Innovationstreiber“. Bei der Einführung neuer Technologien in der Truppe müsse das Thema Resilienz von Anfang an berücksichtigt werden und das Personal entsprechend ausgebildet und geschult werden. Danach gab Bernd Geisler, Präsident des Landesamts für Sicherheit in der Informationstechnik (LSI), einen Einblick in die „Cyber-Resilienz in Bayern“.

Er betonte insbesondere, wie wichtig es ist, auf einen Cybersicherheitsfall vorbereitet zu sein. Neben vorbeugenden Maßnahmen sind daher auch regelmäßige Übungen unerlässlich, die im Voraus klären, wie im Krisenfall zu handeln ist. Zu diesem Zweck wird das LSI künftig mit dem FI CODE an der Entwicklung und Integration realer Cyber-Sicherheitsvorfälle in Cyber-Range-Trainings arbeiten. Das Bundesamt für Sicherheit in der Informationstechnik ergänzte die föderale Perspektive in seinem Vortrag. Dr. Uwe Klapproth hob die Wichtigkeit gesamtstaatlicher Kooperation hervor und zeigte am Beispiel der Übungsserie LÜKEX, wie Bund und Länder den Ernstfall proben. „Mit kluger Resilienz, gemeinsamer Verantwortung und entschlossener Führung können wir den Wettlauf gestalten – nicht nur reagieren“, so Klapproth.

Panel zum Cyber Resilience Act

Prof. Dr. Dennis-Kenji Kipker vom cyberintelligence.institute eröffnete mit seinem Vortrag „Warum Security by Design ein Zukunftsthema ist!“ die zweite Hälfte des Nachmittags. Gleichzeitig leitete er damit auch thematisch zur anschließenden Paneldiskussion über. Unter der Moderation von Oberstleutnant Katja Büchner (Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR), diskutierte Prof. Kipker zusammen mit Andreas Witt (Sopra Steria SE), Sabine Griebsch (GovThings), Silvia Reischer (Swiss Institute for Global Affairs) und Andre Hinüber (Airbus Defence and Space) über das Thema „Der Cyber Resilience Act (CRA): Chance oder Risiko für proaktive Resillienzstrategien?“. Bei der Frage, ob der CRA einen limitierenden Charakter hat oder ein Katalysator für notwendige Entwicklungen sein kann, waren sich die Panellisten mehrheitlich einig und „brachen eine Lanze“ für den CRA – trotz gewisser Herausforderungen, die diskutiert

Viele Gespräche über die Zukunft der Cybersicherheit auf der Jahrestagung CODE 2025: Auf dem Panel diskutieren Prof. Dennis-Kenji Kipker, Andre Hinüber, Sabine Griebsch, Silvia Reischer, Andreas Witt und Oberstleutnant Katja Büchner (v. l. n. r.) zum Cyber Resilience Act der EU.

Generalleutnant Michael Vetter (hintere Reihe, 5.v.l.) und Volker Eiseler (hintere Reihe, r.), beide BMVg, und Prof. Dr. Wolfgang Hommel (hintere Reihe, 2.v.r.) zusammen mit den Finalisten der Innovationstagung Cyber/IT.

wurden. Ebenso sahen die Expertinnen und Experten im CRA eine Chance, Aufmerksamkeit für eine bestehende und viel zu lange vernachlässigte Problematik zu schaffen. Dabei wurde jedoch auch die Gefahr der Überregulierung angesprochen. Zudem wurde über Möglichkeiten und Wünsche zur sicherheitspolitischen Ausgestaltung für den Standort Deutschland gesprochen, bevor die Panellisten letztendlich konkrete Schritte zur Umsetzung aus ihren unterschiedlichen Stakeholder-Perspektiven aufzeigten.

Innovationstagung Cyber/IT

Ein weiterer Höhepunkt war die Innovationstagung Cyber/IT, bei der innovative Konzepte vorgestellt wurden, die das Potenzial haben, die Cyberabwehr nachhaltig zu verbessern. Der Ideenwettbewerb wird nach dem Prinzip „Innovation outside-in“ gemeinsam mit dem BMVg durchgeführt. Aus 38 Einreichungen wählte eine Jury die sieben besten für eine Präsentation aus. In siebenminütigen Pitches stellten die Finalisten ihre Ideen dem Fachpublikum der CODE-Jahrestagung vor. Die Bandbreite der Ideen reichte von KI-gestützter Deception-Technologie, über jammerresistente Navigation durch Multi-Quantensensor-Systeme bis hin zur Schlüsseltechnologie LLLC (Lightweight Low-Latency Consensus) für vertrauenswürdige PNT (Positioning, Navigation and Timing)-Daten in Echtzeit.

Bei der abendlichen Siegerehrung wurden die herausragenden Beiträge gewürdigt und es wurde deutlich, welche Innovationskraft in unserer Community steckt. Dabei konnten Justus Rischke und das Team der Soron Systems die Jury überzeugen. Mit ihrer Idee einer kooperativen Navigation von Drohnenschwärmen in Gebieten, in denen globale Satellitennavigationssysteme, wie beispielsweise GPS, nicht verfügbar oder unzuverlässig sind, holten sie sich den Sieg beim Ideenwettbewerb und sicherten sich damit ein Preisgeld in Höhe von 15.000 Euro. Den zweiten Platz belegte das Team von Styx um Jan Jeske („Maßgeschneiderte analoge KI-Chips – sicher, autark energieeffizient und latenzfrei“) und wurde mit 10.000 Euro belohnt. Den dritten Platz, dotiert mit 5.000 Euro, sicherte sich Martin Rick von der Rick Location Solutions GmbH mit seiner Idee „Where GIS meets EMS – Geospatial Intelligence für das elektromagnetische Spektrum“. Auch die Plätze vier bis sieben konnten sich über ein Preisgeld von jeweils 1.000 Euro freuen. Ihre Urkunden erhielten die Ausgezeichneten am Abend im Rahmen des Social Events von Generalleutnant Michael Vetter. Damit fand der erste Veranstaltungstag seinen Ausklang.

BEIDE ABB.: FI CODE / ANGELIKA WAGENER FOTOGRAFIE

Im Zentrum des Geschehens: Am CODE-Messestand erhielten die Fachbesucherinnen und Fachbesucher aus erster Hand Einblicke in die aktuelle Forschungsarbeit bei CODE.

Vorausschauendes Risikomanagement

Den zweiten Tag der CODE-Jahrestagung 2025 eröffnete Prof. Dr. Michaela Geierhos, Technische Direktorin des Forschungsinstituts CODE. „Die Cyber-Resilienz von morgen verlangt einen Wandel im Denken und Handeln – einen Wandel vom ‚Feuerlöscher-Modus' zum vorausschauenden Risikomanagement.", so Geierhos in ihren einleitenden Worten, die sie mit dem Appell „Lassen Sie uns gemeinsam vordenken, statt nur nachzubessern." abschloss und das Wort an Generalmajor Armin Fleischmann vom Kommando Cyber- und Informationsraum übergab. In seiner Keynote zum Thema „Cyber-Resilienz – Nur wer plant bleibt widerstandsfähig" verdeutlichte der Kommandeur Unterstützung CIR sowie Abteilungsleiter Planung CIR und Digitalisierung der Bundeswehr anhand aktueller Beispiele den Resilienzgedanken und zeigte Lösungsansätze auf. Sein Kerngedanke hierbei: Wer den Schadensfall mit einplant, ist resilient aufgestellt.

Anschließend gaben zwei Professoren des FI CODE Einblicke in ihre aktuelle Forschung. Prof. Dr.-Ing. Mark Manulis, Inhaber der Professur für Privacy, präsentierte aktuelle kryptographische Forschungsansätze zu Verschlüsselung und Authentisierung, um die Sicherheit in Cloud-Umgebungen zu erhöhen. Maximilian Moll, Juniorprofessor für Operations Research – Prescriptive Analytics, stellte seine Forschung zum Quantum Machine Learning vor. In einem lebhaften Vortrag machte der Mathematiker dieses sehr abstrakte und komplexe Zukunftsthema für die Zuhörerschaft zugänglich und verdeutlichte zugleich die derzeitigen Herausforderungen und Ungewissheiten in diesem Themenfeld.

Nach der Kaffeepause ging es mit dem Thema Quantencomputing weiter. In seinem Vortrag mit dem Titel „Quantum Safe und Cyber Resilienz – im Zusammenspiel zum Erfolg" ging Dr. Silvio Dragone von IBM Research auf die drohenden Risiken durch Quantencomputer ein. Diese sind in der Lage, herkömmliche Verschlüsselungsalgorithmen in kurzer Zeit zu knacken. Dragone machte deutlich, wie dringend die Einführung postquantenkryptographischer Standards ist.

Cybersicherheit und Digitalisierung sind Schlüsselfaktoren für eine erfolgreiche Zukunft. Dies hat die Europäische Union früh erkannt und mit „Horizon Europe" und „Digital Europe" zwei Programme aufgelegt, mit denen Forschung und Entwicklung im Bereich Cybersicherheit bzw. Aufbau und Verbreitung digitaler Kapazitäten sowie die praktische Anwendung

BEIDE ABB.: FI CODE / ANGELIKA WAGENER FOTOGRAFIE

innovativer Technologien gefördert werden soll. Dr. Christan Fischer vom DLR Projektträger informierte in seinem Vortrag „Europa? Aber sicher! – Die Rolle des Nationalen Koordinierungszentrums für Cybersicherheit (NKCS)“ über die Arbeit, Vernetzung und das vielfältige Unterstützungsangebot des NKCS, an dem u.a. auch das FI CODE beteiligt ist.

Zu den Vortragenden des zweiten Tages der CODE-Jahrestagung zählte auch Dr. Michael Kissner von der Akhetonics GmbH. Der Gewinner der Innovationstagung Cyber/IT 2023 adressierte in seinem Vortrag “Chip Security & Resilient Semiconductor Supply Chains – Can you Prevent Hardware Backdoors?” die Gefahren von manipulierter Hardware in sicherheitskritischen Systemen. Er zeigte dabei auf, wie insbesondere bei Microchips, die außerhalb von Europa gefertigt werden, unbemerkt Hintertüren (Backdoors) gezielt implementiert werden könnten.

Den Abschluss der Vortragsreihe machte Prof. Dr. Bernhard M. Hämmerli, Professor für Informations- und Netzwerksicherheit an der Hochschule Luzern sowie an der norwegischen University of Science and Technology (NTNU). Mit über drei Jahrzehnten Erfahrung in Forschung, Lehre und Beratung zählt er zu einem der Pioniere der europäischen Cybersicherheitsforschung. In seinem Vortrag „Resilienz – Optimieren der pre-und post-loss Maßnahmen für eine sich ändernde Bedrohungslage“ ging Hämmerli eingangs zunächst auf die grundlegenden Angriffspunkte in der IT ein. Anschließend zeigte er Handlungsoptionen und Entscheidungswege im Falle eines Cyberangriffs auf. Auch zeigte er anhand aktueller Umfragen bei Schweizer Unternehmen auf, wie sie sich auf derartige Vorfälle vorbereiten.

Die Workshop-Themen am Nachmittag des zweiten Veranstaltungstages reichten von Quantentechnologien über vertrauenswürdige KI bis hin zu Serious Games.

Mehr Informationen zur CODE-Jahrestagung

www.unibw.de/code/events/jahrestagungen

www.youtube.com/@FI_CODE

code@unibw.de

Gemeinsam den Herausforderungen der Cybersicherheit begegnen

Nach zwei intensiven Tagen voller inspirierender Vorträge, lebhafter Diskussionen und wertvoller Begegnungen neigte sich die CODE-Jahrestagung langsam ihrem Ende zu. Unter dem Leitthema „Die Cyber-Resilienz von morgen – proaktiv statt reaktiv“ konnte gemeinsam ein Blick in die Zukunft der Cybersicherheit geworfen werden. „Nicht zuletzt möchten wir den Austausch und die Vernetzung hervorheben, die diese Tagung auszeichnen.

Die Gespräche in den Pausen, die Diskussionen nach den Vorträgen und die informellen Treffen haben gezeigt, wie wertvoll der persönliche Kontakt für unsere Arbeit ist.“, betonte Prof. Dr. Michaela Geierhos. „Sei es von der Integration von Quantentechnologien in der Cybersicherheit bis hin zu vertrauenswürdiger KI – die Vielfalt der Workshopthemen spiegelt auch die Komplexität und Dynamik unseres Fachgebiets wider“, sagte Geierhos.

Abschließend dankte sie allen Mitwirkenden an der Jahrestagung – von den Vortragenden über die Fachjury bis hin zu den Sponsoren sowie den zahlreichen helfenden Händen im Hintergrund der Veranstaltung. Auch kündigte Prof. Geierhos bereits die nächste CODE-Jahrestagung für den 14. und 15. Juli 2026 an, bei der auch im kommenden Jahr wieder gemeinsam die Herausforderungen der Cybersicherheit und Lösungen für eine resiliente digitale Zukunft diskutiert werden. ■

Workshop-Bericht von der CODE-Jahrestagung 2025

KI und Führung

In dem international besetzten Workshop wurden Prognosen für die kurzfristige und langfristige Entwicklung der innovativen KI-Technologie charakterisiert und ihre Potentiale im Bereich eines zukunftsweisenden Führungsprozesses identifiziert. Zudem wurden am Ende konkrete Handlungsempfehlungen abgeleitet. Schwerpunkte des Workshops waren die Thematisierung von generativer KI, die Verlässlichkeit und Qualitätssicherung im Hinblick auf komplexe Führungsprozesse und der besondere Aspekt der Charakterisierung von Accountability im Human-in-the-Loop-Prozess.

VON STEFAN PICKL

ALLE ABB.: FI CODE / A. WAGENER

AUSGANGSPUNKT DER DISKUSSION war die schwankende Output-Qualität beim Einsatz von KI-Verfahren sowie die Rolle des Menschen im Human-in-the-Loop-Prozess. Wie können und werden zukünftig Bias, Fairness, Transparenz sowie Daten- und Modellverzerrungen Entscheidungen systematisch beeinflussen? Dadurch sind Erklärbarkeit und Nachvollziehbarkeit – vor allem im Bereich generativer KI – eingeschränkt. Governance und Compliance sowie fragmentierte Regulierungslandschaften (z. B. AI Act, Branchenrichtlinien) treffen zunehmend auf heterogene Toolchains. Ohne klare Policies und Zielvorgaben drohen Schatten-KI, Datensilos und Reputationsrisiken. Die Teilnehmenden waren sich einig, dass Datenschutz und geistiges Eigentum, Nutzung sensibler Daten, Trainingslecks, IP-Fragen bei generierten Inhalten sowie Lieferkettenthemen (Third-Party-Modelle/-APIs) sowohl rechtlich als auch technisch in diesem Kontext anspruchsvoll bleiben werden. In der intensiv geführten Podiumsdiskussion wurden im zweiten Teil des Workshops für diese Kernbereiche einzelne Potentiale und Handlungsempfehlungen abgeleitet: Wenn Menschen „im Loop" bleiben, müssen Rollen, Freigabeschritte und Haftung klar geregelt sein – insbesondere bei sicherheitskritischen oder regulierten Entscheidungen innerhalb von Führungsprozessen. Bias, Fairness, Transparenz und Daten- und Modellverzerrungen können zudem Entscheidungen systematisch benachteiligen.

Folgende Potentiale wurden identifiziert:

- **Bessere Entscheidungen durch Augmentation**
  KI erweitert Wahrnehmung und Optionen (Szenarioanalyse, Risiko-Frühwarnung, Echtzeitanalyse und -optimierung, Hypothesengenerierung), während Menschen Kontext, Werte und Urteilskraft einbringen können.

- **Produktivitäts- und Qualitätsgewinne**
  Automatisierte Synthesen, Drafting, Summarization und Assistant-Funktionen beschleunigen die komplexe Wissensarbeit und heben die Qualität repetitiver oder datenintensiver Aufgaben.

- **Demokratisierung von Analytik**
  Natural-Language-Interfaces und GenKI senken die Eintrittsbarrieren für komplexe Analysen („Self-Service-BI++") – insbesondere hilfreich für Führungskräfte, die schnell tragfähige Einsichten brauchen.

- **Organisationales Lernen**
  Durch Feedback-Schleifen in Human-in-the-Loop-Prozessen entstehen dynamische Wissensbasen und bessere Entscheidungsheuristiken.

In der Diskussionsrunde und in den sich anschließenden Statements wurde vor allem auf die Systematisierung eines Capability-Aufbaus fokussiert, bei dem CODE eine zentrale Rolle zukommen könnte. Auch ein zukunftsweisendes Operation Model sowie Living Lab für Human-in-the-Loop wurde vorgeschlagen.

Offen wurde am Ende der Aspekt diskutiert, wie eine KI-Governance und entsprechende Policies langfristig etabliert werden können. Als Leitbild könnten hier die Aspekte „Augmentation statt Substitution", „transparente Nutzen-/Risiko-Narrative", „Beteiligung der Mitarbeitenden" sowie die „Charakterisierung und Analyse von messbaren Vertrauensindikatoren" dienen. Das sind Themenfelder, an denen bei CODE im internationalen Kontext bereits gearbeitet wird. Der Austausch soll bei der CODE-Jahrestagung 2026 fortgesetzt werden. ■

Unter der Leitung von Prof. Dr. Stefan Pickl (m.) diskutierten Juniorprof. Dr. Maximilian Moll (l.) und Prof. Dr. Bernhard Hämmerli (r.), Mitglied der Schweizerischen Akademie der Technischen Wissenschaften, zusammen mit den Workshop-Teilnehmenden.

Das erste IBM Quantum System Two in Europa, am IBM-Euskadi Quantum Computational Center in San Sebastián, Spanien.

Quantentechnologien

Grundlagenforschung als Voraussetzung für neue Quantenanwendungen

Quantentechnologien gelten als eine der vielversprechendsten und potenziell disruptivsten Entwicklungen unserer Zeit. Sie versprechen weitreichende Auswirkungen auf Verteidigung, Wissenschaft und Industrie – von neuartigen Sensoren über sichere Kommunikationsverfahren bis hin zu leistungsfähigen Quantencomputern.

VON SABINE TORNOW

INHALTLICH LASSEN SICH im Bereich der Quantentechnologien drei zentrale Fähigkeitsbereiche unterscheiden: Navigation und Zeitmessung, Kryptographie, Sensorik sowie Computing. Im Bereich Navigation und Timing ermöglichen Quantensensoren und hochpräzise Atomuhren neue Formen GPS-unabhängiger Positions- und Zeitbestimmung, was die Missionssicherheit in komplexen Einsatzumgebungen erhöhen kann. Im Bereich elektromagnetischer Sensorik und Bildgebung eröffnen quantenbasierte Detektoren Möglichkeiten zur robusteren und präziseren Datenerfassung. Im Bereich Computing stehen langfristige Potenziale im Vordergrund, etwa Material- und Chemiesimulation, die Optimierung komplexer logistischer Prozesse, Auswertung von Quantendaten oder Verbesserungen bei KI-Modellen. Dabei ist zu betonen, dass viele dieser Konzepte bislang nicht im Einzelnen bewiesen sind – das Disruptionspotenzial ist gleichwohl hoch.

Aus militärischer Perspektive variiert der Reifegrad der Technologien erheblich. Große fehlertolerante Quantencomputer sind noch weit von praktischer Einsatzfähigkeit entfernt. Quantensensoren und Atomuhren hingegen befinden sich in einem mittleren Reifestadium und sind einer möglichen Integration deutlich näher.

Die Rolle der Grundlagenforschung

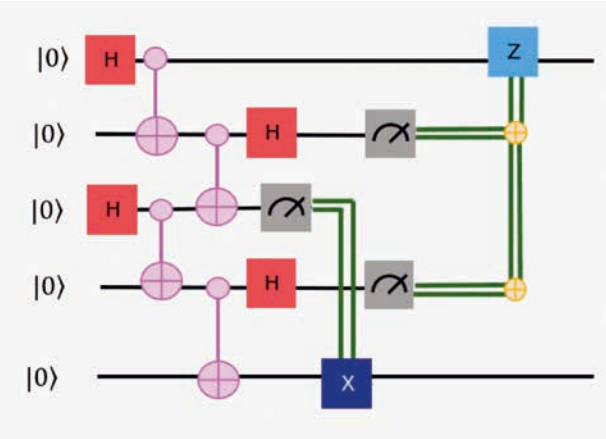
Trotz erheblicher Fortschritte in der Hardwareentwicklung befinden sich viele Quantensysteme noch im experimentellen Stadium. Leistungsfähige, fehlertolerante Quantencomputer existieren bislang nicht, und für zahlreiche der diskutierten Anwendungen fehlt der belastbare Nachweis eines praktischen Vorteils gegenüber klassischen Verfahren. Genau hier setzt die Grundlagenforschung an. Ohne sie lassen sich weder neue, realistische Anwendungsfelder identifizieren noch verlässliche Aussagen über tatsächliche Leistungsgewinne treffen. Grundlagenforschung im Quantum Computing beschäftigt sich nicht mit kurzfristigen Produktentwicklungen, sondern mit den fundamentalen physikalischen, mathematischen und informationstheoretischen Prinzipien der Quanteninformationsverarbeitung. Sie untersucht die Eigenschaften von Qubits, die Grenzen von Kohärenz und Fehlertoleranz, die Struktur von Quantenalgorithmen sowie die Bedingungen, unter denen ein quantenmechanischer Vorteil überhaupt möglich ist.

Erst durch dieses tiefgehende Verständnis lassen sich tragfähige Strategien für skalierbare Systeme entwickeln und potenzielle Anwendungen kritisch bewerten. Bevor Quantencomputer praktische Probleme in der Kryptographie, der Materialforschung oder der Optimierung lösen können, müssen grundlegende Fragen zur Stabilität, Skalierbarkeit, Fehlerkorrektur und zum algorithmischen Vorteil geklärt werden. Grundlagenforschung ist damit keine Vorstufe der Anwendung, sondern ihre Voraussetzung. Sie schafft das wissenschaftliche Fundament, auf dem zukünftige technologische Durchbrüche erst möglich werden.

Notwendig sind neue Qubit-Materialien, skalierbare Architekturen, innovative Algorithmen sowie die Analyse der fundamentalen Informationsgrenzen. Anwendungen müssen in vielen Fällen erst entdeckt werden; sie ergeben sich nicht automatisch aus vorhandener Hardware. Nur durch ein tiefes Verständnis physikalischer Phänomene (Interferenz, Verschränkung und Messung), algorith-

IBM Quantencomputer

BEIDE ABB.: IBM



Dynamische Schaltkreise mit Zwischenmessung und Reset.

mischer Strukturen und neuer Paradigmen lassen sich neuartige Anwendungen identifizieren, bewerten und letztlich operationalisieren.

Im Bereich der Quantenalgorithmik besteht die zentrale Herausforderung heute nicht allein darin, theoretisch interessante Verfahren zu formulieren, sondern diese auch unter realistischen Bedingungen auf fehleranfälliger Quantenhardware zu implementieren. Grundlagenforschung in diesem Kontext bedeutet, neue Rechenparadigmen zu entwickeln, die physikalische Dynamik, Rauschen, Messprozesse und begrenzte Kohärenzzeiten nicht als Störfaktoren behandeln, sondern systematisch in die algorithmische Struktur integrieren.

Quanten-Walks stellen eine quantenmechanische Verallgemeinerung klassischer Random Walks auf Graphen dar. Während klassische Prozesse diffusive Ausbreitung zeigen, entstehen im Quantenfall durch Interferenz nichtklassische Dynamiken, die unter geeigneten Bedingungen zu Beschleunigungen führen können. Ein zentraler algorithmischer Zugang ist die Untersuchung der First Hitting Time: Dabei wird analysiert, wie lange es im Mittel dauert, bis ein bestimmter Zielzustand erstmals detektiert wird, und wie diese Zeit von der Spektralstruktur des zugrunde liegenden Graphen oder Hamiltonians abhängt.

Anders als im klassischen Fall ist die Definition eines „Treffens“ im Quantenfall nicht trivial, da jede Messung den Zustand verändert. In unserer Forschung werden solche Prozesse sowohl theoretisch als auch experimentell auf programmierbarer Quantenhardware untersucht. Durch die Implementierung von Mid-Circuit-Messungen lassen sich First-Hitting-Statistiken direkt aus realen Messdaten extrahieren. [1]

Parallel dazu untersuchen wir **Quantum Reservoir Computing** als besonders hardwarenahen Ansatz für maschinelles Lernen und Zeitreihenprognose. Das Grundprinzip besteht darin, die natürliche Dynamik eines Quantensystems als nichtlineares Reservoir zu nutzen: Eingangsdaten werden in das System eingespeist, die interne Dynamik transformiert sie in einen hochdimensionalen Zustandsraum, und trainiert wird lediglich die Ausleseeinheit. Im Gegensatz zu variationalen Quantenalgorithmen oder parametrischen Quantennetzen muss somit nicht das gesamte System optimiert werden. Der Trainingsaufwand reduziert sich erheblich, und gleichzeitig können komplexe zeitliche Muster verarbeitet werden. Besonders vielversprechend ist dieser Ansatz, weil er bereits mit der derzeit verfügbaren, noch fehleranfälligen Quantenhardware leistungsfähige Berechnungen ermöglicht.

Ein wesentliches Forschungsergebnis besteht in der Entwicklung eines Protokolls zur effizienten Feedback-Verarbeitung in Quanten-Reservoirs. Bisherige Ansätze waren entweder sehr zeitaufwendig oder erlaubten keine Rückkopplungsschleifen, was die Verarbeitung zeitlicher Korrelationen einschränkte. Unser neues Protokoll integriert Feedback-Verbindungen direkt in den kontinuierlichen Quantenprozess: Durch den Einsatz sogenannter Dynamic Circuits mit Mid-Circuit-Messungen und unmittelbarem Feedforward kann das System Informationen innerhalb der Kohärenzzeit eines Qubits verarbeiten und sich an vergangene Eingaben „erinnern“, ohne den Rechenvorgang zu unterbrechen. Diese Architektur erhöht signifikant die Speicherkapazität und Vorhersagekraft des Reservoirs bei gleichzeitig hoher Verarbeitungsgeschwindigkeit. Die Fähigkeit zu schnellen Feedback-Schleifen ist zudem auch für zukünftige Quantenfehlerkorrekturprotokolle von zentraler Bedeutung. [2]

Ein grundlegend neues Rechenparadigma ergibt sich aus der Übertragung des **stochastischen Rücksetzens** in die Quantenwelt. In der klassischen statistischen Physik und Informatik ist **Resetting** ein etabliertes Prinzip: Bei diffusionsartigen oder randomisierten Suchprozessen kann eine optimale Reset-Rate dazu führen, dass eine sonst divergierende mittlere Erstpassagezeit endlich wird – ein Konzept, das auch in randomisierten Algorithmen und Monte-Carlo-Methoden routinemäßig genutzt wird. In der Quantenmechanik wird dieses Prinzip grundlegend erweitert, da Kohärenz, Verschränkung und Messrückwirkung eine neue Qualität hinzufügen: Jeder Reset wirkt als Mess- und Präparationsschritt, der den Quantenzustand verändert. Das Zusammenspiel von unitärer Dynamik und gezielten nichtunitären Eingriffen ermöglicht so nichtklassische Beschleunigungen, die im klassischen Resetting kein Gegenstück haben.

Ergänzend widmet sich ein weiterer Teil unserer Forschung der grundlegenden Steuerung von **Quantenvielteilchensystemen** fernab des thermischen

ABB.: IBM / SIMONE CANTORI; IBM

Gleichgewichts. In einer experimentellen Studie auf programmierbarer Quantenhardware konnten wir zeigen, dass gezielte, stochastische Rücksetzungen stabile und kontrollierte Zustände in wechselwirkenden Qubitsystemen erzeugen können. Dazu wurde ein theoretisches Modell entwickelt, das Messprozesse, und nichtunitäre Dynamik präzise beschreibt; dieses Modell wurde experimentell validiert. Die Ergebnisse etablieren das stochastische Rücksetzen als neue Basismethode, um komplexe Quantendynamiken gezielt zu steuern, metastabile Regime zu stabilisieren und kontrollierte Zustände für algorithmische Anwendungen bereitzustellen. [3]

Insgesamt zeigt sich, dass Grundlagenforschung im Bereich der Quantenalgorithmik heute weit über die Konstruktion idealisierter, tiefer Schaltkreise hinausgeht. Sie umfasst die Entwicklung dynamikbasierter Rechenmodelle, die systematische Integration von Messung und Feedback, die Analyse von Zeit-zu-Ereignis-Strukturen im Quantenfall sowie die Nutzung Nichtgleichgewichtsdynamik als algorithmische Ressource. Die drei vorgestellten Forschungsrichtungen – Quantum-Walk-basierte First-Hitting-Time-Analyse, Quantum Reservoir Computing mit integriertem Feedback und stochastisches Rücksetzen – verdeutlichen, wie fundamentale Theorie, experimentelle Hardware und algorithmische Innovation zusammengeführt werden können.

Diese Arbeiten definieren nicht nur neue Anwendungswege, sondern tragen grundlegend dazu bei, zu verstehen, was Rechnen im quantenmechanischen Sinne bedeutet und unter welchen physikalischen Bedingungen ein belastbarer Vorteil realisiert werden kann. ■

PUBLIKATIONEN

Literatur zu 1

LIU Q., TORNOW, S., KESSLER, D. A., BARKAI, E.: Fractionally quantized recurrence detection times in monitored quantum many-body systems. Proceedings of the National Academy of Sciences 123 (22), e2529694123.

HEINE, T., BARKAI, E., ZIEGLER, K., TORNOW, S.: Quantum walks: First hitting times with weak measurements. Physical Review A 113 (5), 052426.

ZIEGLER, K., HEINE, T., TORNOW, S.: Monitoring of quantum walks with weak measurements. arXiv preprint arXiv:2603.26933.

MA, S., TORNOW, S., BARKAI, E.: Resonances, Recurrence Times and Steady States in Monitored Noisy Qubit Systems. arXiv preprint arXiv:2603.18996.

YIN, R., WANG, Q., TORNOW, S., BARKAI, E.: Resonances of recurrence time of monitored quantum walks. The Journal of Chemical Physics 162 (24).

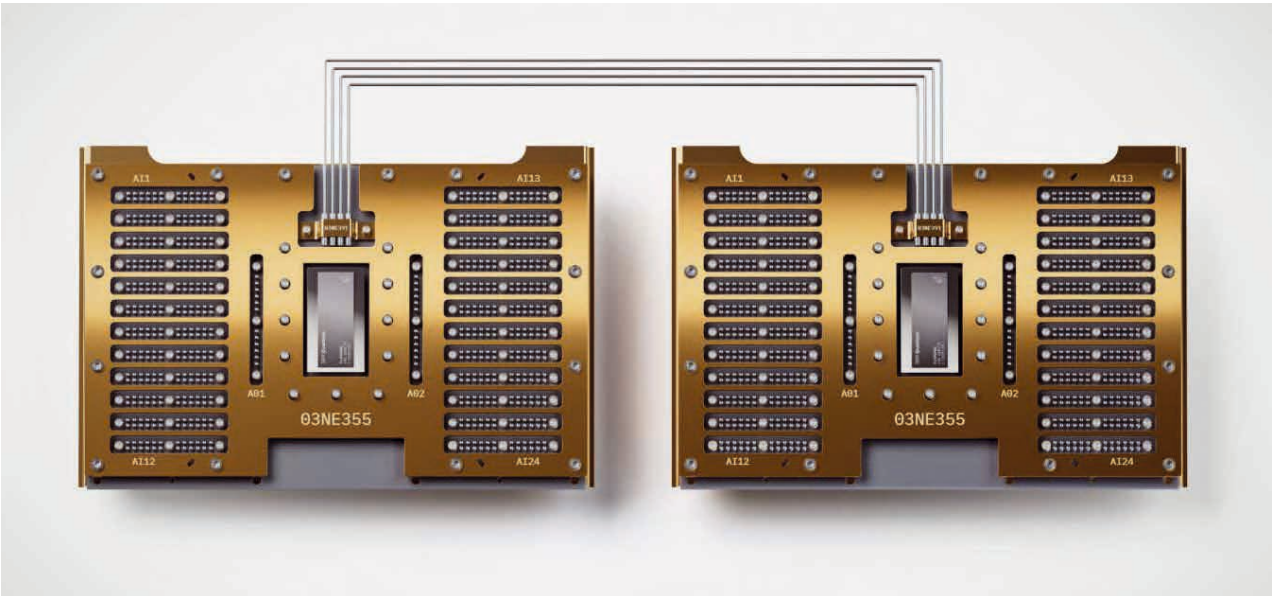
YIN, R., WANG, Q., TORNOW, S., BARKAI, E.: Restart uncertainty relation for monitored quantum dynamics. PNAS 122 (1), e2402912121.

Literatur zu 2

MURAUER, J., KRISHNAKUMAR, R., TORNOW, S., GEIERHOS, M.: Feedback connections in quantum reservoir computing with mid-circuit measurements. 2025 IEEE International Conference on Quantum Computing and Engineering (QCE).

Literatur zu 3

MURAUER, J., TORNOW, S., PERFETTO G.: Nonequilibrium steady states induced by stochastic mid-circuit measurements and resets on a quantum computer. arXiv:2606.19027.



Modulares Quantencomputing.

ABB.: ADOBE STOCK / KAIHKOIMAGES

Nationales Koordinierungszentrum für Cybersicherheit Deutschland

Forschungsbedarf im Bereich Cybersicherheit im deutschen Verteidigungssektor

Gemeinsame Untersuchungen zur Stärkung der Cybersicherheit und zur Gewährleistung der digitalen Souveränität Deutschlands

VON CORINNA SCHMITT

CYBERSICHERHEITSUNTERSUCHUNGEN sind in der heutigen digitalen Landschaft von entscheidender Bedeutung, insbesondere für den deutschen Verteidigungssektor, der zunehmend komplexen Cyberbedrohungen durch staatliche und nichtstaatliche Akteure ausgesetzt ist. Da sich die moderne Kriegsführung auf den Cyberspace ausweitet, stellen Angriffe auf kritische Infrastrukturen, militärische Netzwerke und verteidigungsbezogene Technologien eine direkte Bedrohung für die nationale Sicherheit und die Einsatzbereitschaft dar. Durch zeitnahe und gründliche Cyber-Untersuchungen können Schwachstellen identifiziert, Angriffe zugeordnet und wirksame Gegenmaßnahmen ergriffen werden – so kann Deutschland nicht nur seine physischen Grenzen, sondern auch seine digitale Souveränität verteidigen. Ebenso wichtig ist die Einführung eines Dual-Use-Ansatzes, der zivile und militärische Fähigkeiten miteinander verbindet. Zivile Sektoren

sind oft führend in Sachen Innovation, Geschwindigkeit und Anpassungsfähigkeit, während das Militär robuste Sicherheitsprotokolle, strategische Informationen und umfangreiche Ressourcen bereitstellt. Durch die Integration dieser Stärken kann Deutschland eine widerstandsfähige, agile und zukunftssichere Cyberabwehr aufbauen. Die Zusammenarbeit zwischen zivilen Forschungseinrichtungen, privaten Technologieunternehmen und militärischen Behörden fördert eine ganzheitliche und einheitliche Cybersicherheitsstrategie, die für die Sicherheit des Landes in einer Zeit, in der die Grenze zwischen Frieden und Konflikt durch digitale Operationen zunehmend verschwimmt, von entscheidender Bedeutung ist.

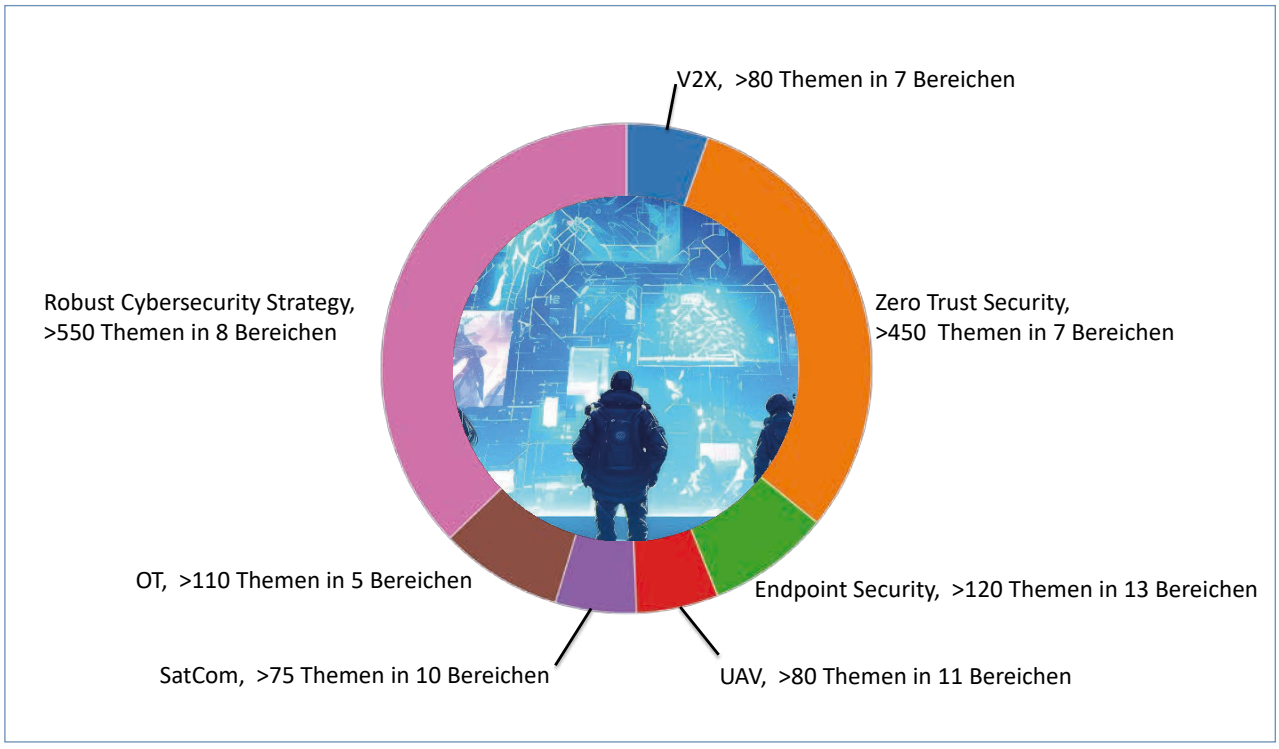
So untersuchte FI CODE als Teil des Nationalen Cybersicherheits-Koordinierungszentrums Deutschland über einen Zeitraum von 30 Monaten, welche Themen für die deutsche Verteidigung von Interesse sind. Die Ergebnisse sind Teil des zugehörigen Projekts NCC-DE, das im Rahmen des EU-Programms „Digitales Europa“ (DIGITAL) unter der Nr. 101126787 gefördert wird. Akteure aus Wissenschaft, Forschungseinrichtungen, KMU und Industrie aus verschiedenen Anwendungsbereichen wie Automobil, Gesundheit, Bauwesen, Luftfahrt, Raumfahrt, Logistik und kritische Infrastrukturen erklärten übereinstimmend, dass eine scharfe Trennung zwischen zivilen und militärischen Bereichen in der Cybersicherheit und bei Untersuchungen nicht mehr sinnvoll ist und sogar hinderlich sein kann. Sie bevorzugen eindeutig den Dual-Use-Ansatz und sehen darin klare Vorteile. Diese Integration nutzt zivile Innovationen, Geschwindigkeit und Anpassungsfähigkeit sowie militärische Sicherheitsprotokolle, strategische Informationen und Ressourcen, um eine widerstandsfähige, agile und zukunftssichere Cyberabwehrhaltung zu schaffen. Die Zusammenarbeit zwischen zivilen Forschungseinrichtungen, privaten Technologieunternehmen und militärischen Einrichtungen wird als entscheidend für eine ganzheitliche und einheitliche Cybersicherheitsstrategie angesehen.

Zusammenfassend lässt sich sagen, dass konkrete Anwendungsbereiche – Vehicle-to-Everything (V2X), Zero Trust Security, Endpoint Security, Satellitenkommunikation (SatCom) und unbemannte Luftfahrzeuge (UAV) – sowie eine globale Strategie mit Schwerpunkt auf einer robusten Cybersicherheitsstrategie und der Sicherheit der Betriebstechnologie (OT) untersucht werden müssen. Darüber hinaus wurden diverse Bereiche thematisiert, wie die Kryptographie, Kommunikation, Netzwerkinfrastruktur, Cloud-Dienste, der Datenaustausch sowie Schulungen und Entwicklungen im Bereich der Reaktion auf Vorfälle und Standardisierung. ■

PD Dr. Corinna Schmitt

corinna.schmitt@unibw.de

https://www.nkcs.bund.de/



Schematische Aufteilung des Forschungsbedarfs im deutschen Verteidigungssektor.

ABB.: FI CODE / C. SCHMITT; FOTO: ADOBE STOCK / YANLONG

Gruppenfoto der anwesenden Teilnehmer und Teilnehmerinnen der DigiTwin 2025.

Bericht zur DigiTwin-Konferenz 2025 in Garmisch-Partenkirchen

Digitale Zwillinge optimieren die Welt

Vom 14. bis 18. Oktober 2025 fand in Garmisch-Partenkirchen die fünfte internationale Konferenz zum Thema „Digital Twin“ statt. Unter dem Sonderthema „Digital Twin Optimizing the World“ versammelten sich führende Forscherinnen und Forscher sowie Industriepartner, um neue Ergebnisse auszutauschen, Grenzen zu diskutieren und eine high-level Plattform für den internationalen Austausch zu schaffen.

VON STEFAN PICKL

DIGITALE ZWILLINGE (*digital twins*) haben sich von einem konzeptionellen Rahmen zu einem ausgereiften Forschungs- und Ingenieurparadigma entwickelt, das in vielen Bereichen, insbesondere in cyber-physischen Systemen, messbaren wissenschaftlichen und praktischen Nutzen bringt. Durch die Abstimmung von Modellen, Daten und Steuerung in einem geschlossenen Regelkreis erhöhen sie die Zuverlässigkeit und Qualität, verkürzen die Vorlaufzeit, senken Kosten und Energieverbrauch und stärken insbesondere die Sicherheit und Widerstandsfähigkeit (*resilience*).

In diesem Zusammenhang fand vom 14. bis 18. Oktober 2025 in Garmisch-Partenkirchen die fünfte internationale Konferenz zum Thema „Digital Twin" statt. Unter dem Sonderthema „Digital Twin Optimizing the World" versammelten sich führende Forscherinnen und Forscher sowie Industriepartner, um neue Ergebnisse auszutauschen, Grenzen zu diskutieren und eine high-level Plattform für den internationalen Austausch zu schaffen, die Innovationen in der Wissenschaft und Technik der digitalen Zwillinge vorantreibt. Das hybride Programm umfasste drei Veranstaltungsorte für die persönliche Teilnahme sowie 21 Online-Veranstaltungen, bot 226 akademische Vorträge und zog mehr als 1.200 Teilnehmer aus über 20 Ländern an.

Digitale Zwillinge zur Optimierung intelligenter Städte

Städte sind komplexe und voneinander abhängige Systeme, die durch menschliches Verhalten und Politik geprägt sind. Digitale Zwillinge synchronisieren die Erfassung, Modellierung und Steuerung von Energie, Verkehr, Wasser und Gebäuden, um öffentliche Dienstleistungen durch Echtzeitanalysen und datengetriebene Optimierung zu verbessern. Durch die Integration von Nachfrage-, Zustands- und Umweltdaten in einheitliche Modelle ermöglichen digitale Zwillinge genaue Prognosen und adaptive Steuerung für Verkehrssysteme, Gebäudeautomation und dezentrale Energieversorgung, während die Zuverlässigkeit durch Anomalieerkennung und Korrekturmaßnahmen verbessert wird.

Die Stadtplanung profitiert von detaillierten Szenarioanalysen, die Strategien auf Resilienz, Fairness und Emissionen testen, und in Notfällen leiten digitale Zwillinge die Evakuierung und die Zuweisung von Ressourcen. Modelle auf Gebäudeebene unterstützen die modellbasierte Steuerung, während Stadtteile sich „koordinieren", um die Last auszugleichen und gleichzeitig erneuerbare Energien integrieren; die Bürger gewinnen an Transparenz, da Leistung und Entscheidungen datenbasiert und nachvollziehbar werden. Mit diesen digitalen Fähigkeiten können Städte Emissionen und Verzögerungen reduzieren und gleichzeitig die Sicherheit und die Gleichheit der Dienstleistungen verbessern. Darüber hinaus wurden während der Konferenz Digitale Zwillinge zur Optimierung des Gesundheitswesens, der Luftfahrt, von Transport und Logistik sowie cyber-physischer Systeme diskutiert.

Echtzeitoptimierung und Sicherheitsbeschränkungen

Die zentrale Herausforderung besteht in der Schaffung von skalierbaren Echtzeit-Digital-Twin-Loops, die unter Ressourcenbeschränkungen und Sicherheitsauflagen zuverlässig die Realität abbilden. Zu den Forschungsschwerpunkten gehören die robuste Datenassimilation aus spärlichen oder verzögerten Eingaben, die multiskalare Modellierung mit validierten Fehlergrenzen und die hierarchische Steuerung mit expliziten Garantien hinsichtlich Latenz und Sicherheit. Laufzeitmetriken sollten Latenz, Durchsatz, Genauigkeit und Ressourcennutzung quantifizieren. Für Fortschritte sind realistische Datensätze, offene Plattformen und interaktive Testumgebungen (Living Labs) erforderlich, die eine reproduzierbare Bewertung und datengesteuerte Optimierung ermöglichen.

Standards, Ethik und Governance

Da digitale Zwillinge die Ergebnisse in der physischen Welt beeinflussen, müssen Standards und Governance auch Transparenz und Verantwortlichkeit gewährleisten. Gemeinsame Metadaten und Formate sollten den Transfer von Modellen zwischen verschiedenen Umgebungen ermöglichen, während eine ethische Legitimierung die Erkennung von Verzerrungen, die Offenlegung von Unsicherheiten und klare Gültigkeitsgrenzen erfordert. Governance sollte die Datenverantwortung, die Kontrolle von Modelländerungen und Prüfpraktiken definieren, während die Zertifizierung strenge Testverfahren und Berichtsstrukturen erfordert, die die operative Expertise widerspiegeln.

Hauptredner waren u. a. Juniorprof. Dr. Maximilian Moll, Prof. Dr. Bernhard Hämmerli (Schweizerische Akademie der Technischen Wissenschaften) und Honorarprofessor General (a. D.) Dr. Dr. Dieter Budde. Juniorprof. Dr. Moll erhielt eine Auszeichnung für die beste Präsentation. Vorsitzender der Konferenz war Prof. Dr. Stefan Pickl. HOLM und das Forschungszentrum RISK waren Partner der Konferenz, die zum ersten Mal in Deutschland stattfand. Die nächste DigiTwin-Konferenz wird im August 2026 an der Universität Oxford stattfinden. ■

ABB.: UNIBW M / S. PICKL

MERLIN

Blackout-taugliche Kommunikations-infrastruktur für Krisensituationen

Regionale Katastrophen wie Extremwetterereignisse gehen oft mit der Zerstörung öffentlicher Infrastruktur einher. Wenn in tagelang von der Außenwelt abgeschnittenen Ortschaften Strom, Mobilfunk und Internet-Zugang ausfallen, wird die Lagebeurteilung durch Einsatzkräfte mangels direkter Kommunikation mit den Betroffenen massiv erschwert. Mit MERLIN wurde ein Forschungsprototyp zur autarken Notfallkommunikation per LoRa-Funk in der Kärtner Gemeinde Neuhaus in Betrieb genommen.

VON MARIO SILACI

IM SOMMER 2023 zerstörte ein länger anhaltendes Starkregenereignis mit Erdrutschen mehrere Straßen und Brücken im Gebiet der Gemeinde Neuhaus. Durch die mittelgebirgige Lage im Grenzgebiet zu Slowenien und starke Bewaldung konnten ganze Ortsteile und zahlreiche kleinere Siedlungen auch von Einsatzkräften nicht mehr zeitnah und ohne Selbstgefährdung erreicht werden. Durch inhärent suboptimale Mobilfunkversorgung im betroffenen Gebiet und zerstörte Telefonleitungen war kein direkter Kontakt möglich, um beispielsweise Hilfsmaßnahmen auf akute lebensbedrohliche Notfälle zu fokussieren.

Über gemeinsame Kontakte im Österreichischen Bundesheer, das die Krisenbewältigung 2023 unterstützte, entstand eine Kooperation mit dem am FI CODE durchgeführten dtec.bw-Projekt ROLORAN, das zivile und militärische Anwendungen der Funktechnologie LoRa in technisch herausfordernden Umgebungen untersucht. Mit MERLIN („Messaging mit regionaler LoRa-Infrastruktur“) wurde im September 2025 die zweite Generation eines Forschungsprototyps in zehn Ortschaften des Gemeindegebiets Neuhaus in den Langzeit-Testbetrieb überführt.

Kommunikation zwischen Bevölkerung und Krisenstab

MERLIN ermöglicht den textbasierten Nachrichtenaustausch zwischen einem von der Gemeinde eingerichteten Krisenstab und den Betroffenen sowie mobilen Einsatzkräften. In Neuhaus spannen dafür zehn stationäre MERLIN-Basen ein Funk-Mesh-Netz-

ALLE ABB.: FI CODE / DR. MICHAEL GRABATIN

Demonstration von MERLIN im Rahmen eines Expertenworkshops.

Vorstellung von MERLIN bei der Pressekonferenz in Neuhaus.

werk über das gesamte Gemeindegebiet auf. Grundlage der MERLIN-Basen sind umgebaute Telefonzellen, die mit im Projekt entwickelten Elektronikkomponenten und eigener Software ausgestattet wurden. Integrierte E-Ink-Monitore stellen eingehende Nachrichten dar und ermöglichen zusammen mit einer angeschlossenen Tastatur das angeleitete Versenden von Notfallmeldungen und Mitteilungen. Alle MERLIN-Basen werden mithilfe von Photovoltaik-Elementen mit Strom versorgt und verfügen über einen Batteriepuffer, der mehrere Wochen ohne nennenswerte Sonneneinstrahlung überbrücken kann.

Mit vergleichbarer Funktionalität sind die mobilen MERLIN-Messenger für Haushalte und Einsatzkräfte ausgestattet. Sie können mit einer handelsüblichen Powerbank rund zwei Wochen lang durchgehend betrieben werden. Mit Touchscreen, einer kleinen Tastatur und in Smartphone-Größe erlauben sie in Reichweite der MERLIN-Basen das Senden und Empfangen von Nachrichten und können optional auch als mobilen Repeater zur Vergrößerung des vom LoRa-Funk abgedeckten Gebiets eingesetzt werden.

Alle versendeten Nachrichten der MERLIN-Basen und MERLIN-Messenger gehen bei einer Krisenstabsoftware ein. Mit am Computer angeschlossenem MERLIN-Messenger ermöglicht die Software eine Korrespondenz zwischen Krisenstab und MERLIN-Basen/Messengern sowie das Management des LoRa-Funknetzes. Vergleichbar mit E-Mail-Programmen können Nachrichten versendet, empfangen, bearbeitet und annotiert werden, um mit Bürgern oder Einsatzkräften zu kommunizieren und Hilfsmaßnahmen zu koordinieren. Periodisch aktualisierende Übersichtsseiten zum Zustand des gesamten Netzes gewähren eine schnelle Einschätzung der Funktionstüchtigkeit der Infrastruktur und bieten Werkzeuge zur Fernwartung.

MERLIN-Software für den Krisenstab.

Mobilgerät MERLIN-Messenger

Üben für den Ernstfall

Ende September 2025 wurde die MERLIN-Infrastruktur in Neuhaus bei Bürgerinformationsabenden, Expertenrunden sowie einer Pressekonferenz vor Ort präsentiert und erhielt viele positive Rückmeldungen von allen Beteiligten. Seit Oktober 2025 werden regelmäßige Krisenübungen durchgeführt, um Routine aufzubauen und im Ernstfall mit MERLIN einsatzfähig zu sein. Ergebnisse dieser Praxistests unter verschiedenen Witterungsbedingungen und über einen längeren Zeitraum fließen in die weitere Verbesserung des Prototyps ein. Für 2026 ist unter anderem die Integration dezentraler Sensordaten zur weiteren Verbesserung des Lagebilds im Krisenstab geplant.

Wir danken der Gemeinde Neuhaus und allen vor Ort freiwillig Mitwirkenden für die Unterstützung im Langzeit-Testbetrieb!

FOTO: UNIBW M

Ehrung für Stefan Pickl

Aufnahme in den Club of Rome

Am 18. September 2025 wurde Stefan Pickl, Professor für Operations Research an der Universität der Bundeswehr München, zum Mitglied im internationalen Club of Rome ernannt.

VERLIEHEN WURDE DIE ehrenvolle Mitgliedschaft für Pickls Verdienste um die wissenschaftliche Analyse und Modellierung von Krisen- und Konfliktszenarien sowie für die von ihm entwickelten innovativen Lösungsansätze. „Er ist ein Systemdenker mit einem Gespür dafür, Verbindungen zwischen verschiedenen Disziplinen herzustellen – von Elektrotechnik und Philosophie bis hin zu Spieltheorie und Friedensförderung“, schrieb der Club of Rome zu seiner Ernennung.

Ferner würdigte die Organisation sein breites gesellschaftliches und international vernetztes Engagement für den Zivilschutz und den Schutz kritischer Infrastrukturen, etwa als Mitglied im Wissenschaftlichen Beirat des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK), als Mitglied der Deutschen Akademie für Technikwissenschaften (acatech) sowie als Vizepräsident des Deutschen Komitees für Katastrophenvorsorge (DKKV). Prof. Pickl ist überdies Gründungsmitglied des Forschungszentrums Risiko, Infrastruktur, Sicherheit und Konflikt (FZ RISK) an der UniBw M.

Stefan Pickl entwickelte als einer der ersten Wissenschaftler weltweit ein mathematisches Modell zur Modellierung, Analyse und Optimierung des weltweiten CO_2-Zertifikatehandels. Diese Untersuchungen haben auch heute noch große Aktualität und beeinflussen allgemeine Ressourcenkonfliktszenarien und Krisenvorhersagen.

Prof. Pickl arbeitet mit Ernst-Ulrich von Weizsäcker (ehemaliger Co-Präsident des Club of Rome) zusammen und betrachtet den Biochemiker und Systemforscher Frederic Vester (1925 – 2003) als eines seiner Vorbilder. Pickl freut sich besonders darüber, dass Frederic Vester selbst Professor an der UniBw M war und damit die Tradition der „Kunst des Vernetzten Denkens“ in München in besonderer Form fortgesetzt wird. ■

ABB.: ADOBE STOCK / MANKJON

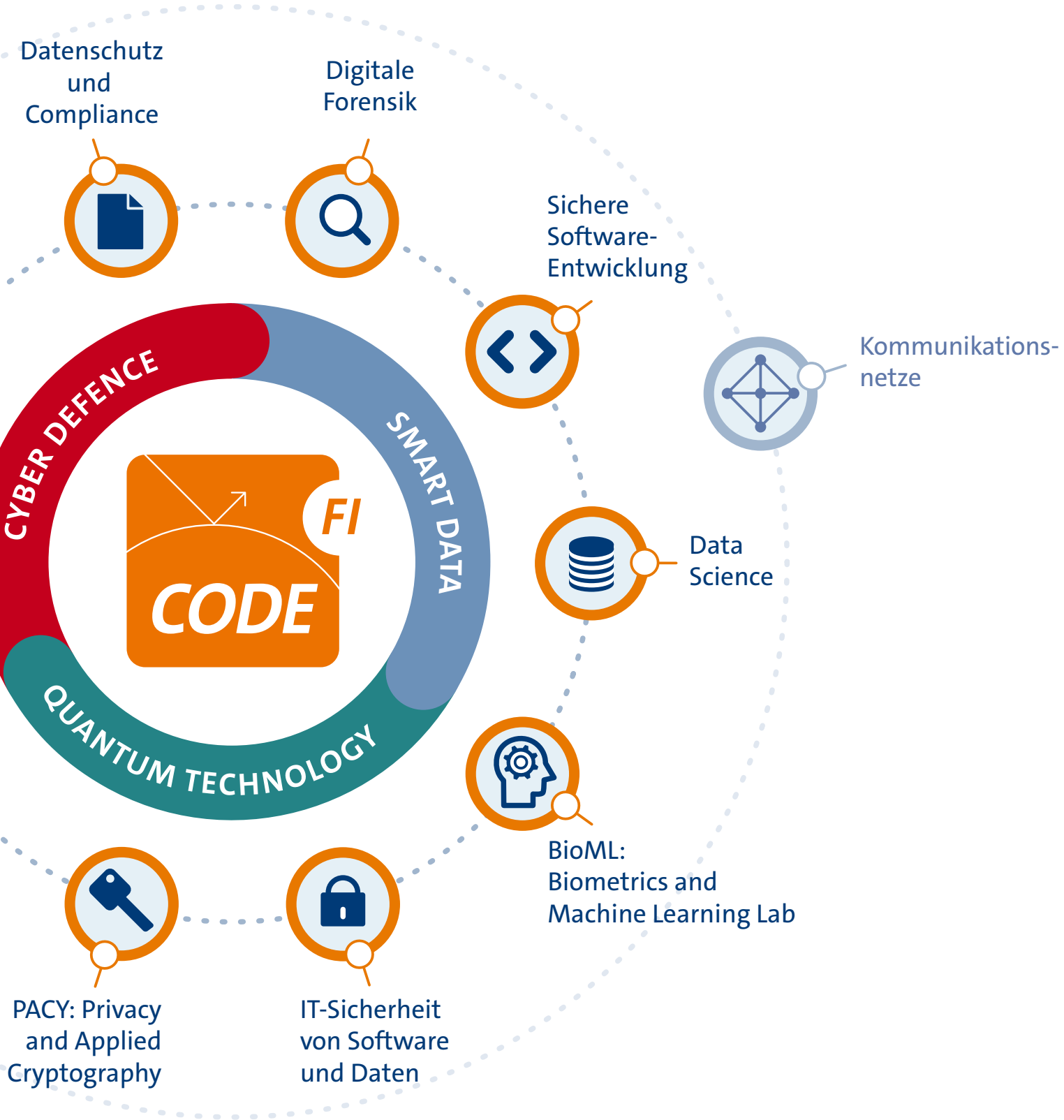
Forschung

Porträts und Projekte

Die Forschung am FI CODE

Am Forschungsinstitut CODE wurden im Jahr 2025 insgesamt 48 drittmittelfinanzierte Projekte in verschiedenen Forschungsgruppen durchgeführt. Eine Auswahl finden Sie auf den folgenden Seiten. Übergreifend forscht CODE in drei Geschäftsbereichen: Cyber Defence, Smart Data und Quantum Technology.

ABB.: TAUSENDBLAUWERK.DE


Datenschutz und Compliance
Digitale Forensik
Sichere Software-Entwicklung
Kommunikations-netze
Data Science
BioML: Biometrics and Machine Learning Lab
IT-Sicherheit von Software und Daten
PACY: Privacy and Applied Cryptography
CYBER DEFENCE
SMART DATA
QUANTUM TECHNOLOGY
FI
CODE

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

Die Forschungsgruppe hat sich über die letzten Jahre besonders im Bereich Software-Defined Defense engagiert. Einladungen zu Vorträgen und Diskussionsrunden bei internationalen Konferenzen als auch renommierte Preise belegen die einzigartige und umfassende Kompetenz der Forschungsgruppe auf diesem Gebiet.

DURCH DIE VERBINDUNG von beruflicher Anerkennung und erfolgreicher Ausrichtung wissenschaftlicher Veranstaltungen erwies sich das vergangene Jahr als außerordentlicher Erfolg für das Munich Computer Systems Research Laboratory (µCSRL).

Aus Projektperspektive wurden 2025 drei große Projekte abgeschlossen: APERITIF, DEMISEC und DEPS. APERITIF bündelte die Forschungsaktivitäten im Bereich der automatisierten Identifikation von Schwachstellen. DEMISEC förderte die Forschung zur Identifikation von Schwachstellen in Binärdateien. DEPS unterstützte die umfangreiche Forschung zum Schutz proprietären geistigen Eigentums durch einen einzigartigen Mechanismus, der eine wirksame Bindung von Software an Hardware ermöglicht.

Die gesamte µCSRL-Forschungsgruppe nahm am 41. Workshop der GI-Fachgruppe für Programmiersprachen und Rechenkonzepte in Bad Honnef teil. Darüber hinaus organisierte Prof. Brunthaler das 23. Kolloquium für Programmiersprachen und Grundlagen der Programmierung in Feldkirchen-Westerham. Das Kolloquium wurde von Friedrich Bauer (TU München), Klaus Indermark (RWTH Aachen) und Hans Langmaack (CAU Kiel) 1982 begründet. Prof. Langmaack konnte an diesem 23. Kolloquium teilnehmen, weshalb insgesamt vier Generationen der „akademischen Familie“ präsent waren (Prof. Langmaack, Prof. Knoop, Prof. Brunthaler, derzeitige µCSRL-Doktoranden).

Das unbestrittene Highlight aus Forschungsperspektive war die Annahme des TEPHRA-Papers bei der 40. IEEE/ACM International Conference on Automated Software Engineering, ASE 2025, einer hochrangigen, äußerst selektiven und prestigeträchtigen Konferenz. TEPHRA gewann außerdem den ACM SIGSOFT Distinguished Paper Award bei der ASE, was die Wertschätzung der wissenschaftlichen Gemeinschaft und die erzielten Ergebnisse unterstreicht.

Zusammenfassend setzte µCSRL seine von Clausewitz'sche Reise fort: „Sprachbasierte Sicherheit ist die Fortsetzung des Compilerbaus *mit anderen Mitteln*.“

Prof. Brunthaler hielt eingeladene Vorträge beim 11. AMSec-Workshop an der Vrije Universiteit Amsterdam, beim Verteidigungsministerium in Berlin und bei der CyCon 2025, der internationalen Konferenz über Cyber-Konflikte in Tallinn, Estland, wo Prof. Brunthaler auch Panelmitglied war. Er war außerdem Jurymitglied beim niederländischen Cybersecurity-Wettbewerb. Darüber hinaus war im ersten Halbjahr 2025 der Gastwissenschaftler Giacomo Priamo von La Sapienza in Rom zu Besuch und führte seine Forschung zu automatisierter Programmreparatur unter Nutzung von PL-Semantik durch.

Die µCSRL-Forschungsgruppe erhielt Förderungen vom deutschen Bundesministerium der Verteidigung, der Österreichischen Forschungsförderungsgesellschaft (FFG), Hensoldt und Oracle Labs.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

www.unibw.de/ucsrl

ABB.: ISTOCK / DE M10

Die Grenzen von Fuzz-Testing-Systemen aufdecken

Semantik-gesteuerte Synthese zur Evaluierung von Fuzzer-Fähigkeiten

TEPHRA ist eine Methodik, die Semantik-gesteuerte Synthese einsetzt, um fehlerfreie Programme mit vielfältigen Hindernissen zu erzeugen und die Fähigkeit eines Fuzzers, diese zu überwinden, statistisch zu bewerten. Die Generierung von 21 Hindernissen sowie die empirische Evaluation der Umgehungsfähigkeit von 31 aktuellen Fuzzern erfolgte mit einem Verbrauch von 37 CPU-Jahren Rechenleistung. TEPHRA deckte Einschränkungen in bestehenden Fuzzing-Heuristiken auf und identifizierte Fehler in den Fuzzern selbst.

Fuzz Testing

Fuzz Testing (oder Fuzzing) wurde 1990 als kostengünstige Testmethode eingeführt, bei der ein Programm mit zufälligen Eingaben versorgt und auf Abstürze überwacht wird. Seitdem hat die Forschung in Industrie und Wissenschaft Fuzzing in eine Technik verwandelt, die etablierte Verifikations- und Validierungsmethoden ergänzt, um die Korrektheit von Programmen zu verbessern. Coverage-geführtes Fuzzing arbeitet heute als stochastischer Prozess, der den Zustandsraum eines Programms abtastet und dabei auf das Auffinden neuer Code- oder Datenfluss-Pfade ausgerichtet ist. Dieser Fortschritt ermöglicht es Coverage-geführten Fuzzern, automatisch Fehler in komplexen realen Systemen wie Webbrowsern, Datenbanken, Betriebssystemen und sicherheitskritischen Bibliotheken zu finden.

Das allgemeine Problem der Programvalidierung und Fehlersuche ist jedoch unentscheidbar. Daher stützen sich Fuzzer auf Heuristiken. Ein Fuzzer ist somit eine Sammlung ad-hoc entwickelter Techniken, die in der Praxis häufig funktionieren, aber in spezifischen Kontexten versagen können. Im Gegensatz zu korrekten und vollständigen Methoden wie abstrakter Interpretation, bounded Model Checking oder interaktivem Theorembeweisen fehlt dem Fuzz Testing eine grundlegende theoretische Basis. Die Wirksamkeit wird ausschließlich anhand empirischer Daten bewertet, darunter Benchmark-Ergebnisse und Resultate aus realen Fuzzing-Einsätzen.

Empirische Beobachtungen zeigen, dass ein Coverage-geführter Fuzzer bei jedem nicht-trivialen Programm schließlich ein Coverage-Plateau erreicht. An diesem Punkt macht er keine Fortschritte mehr, obwohl zusätzliche Coverage möglich wäre. Der Fuzzer erzeugt keine Eingaben, die unerforschte Zustände erreichen, und übersieht dadurch potenzielle Fehler. Mit anderen Worten: Der Fuzzer bleibt stecken. Dennoch fehlt ein systematisches Verständnis oder ein Ansatz, um solche Hindernisse zu überwinden.

Ein neuer Ansatz: TEPHRA

Um dieses Problem anzugehen, wurde TEPHRA entwickelt, eine Methodik zur Bewertung der Fähigkeit eines Fuzzers, schwer erreichbare Programmzustände zu explorieren. Im Gegensatz zu bestehenden Bug-Finding-Benchmarks verfolgt TEPHRA einen grundlegend anderen Ansatz. Die Methodik nutzt pseudorandomisierte, Semantik-gesteuerte Programmsynthese, um Obstacle-Snippets unterschiedlicher Komplexität zu erzeugen, und verwendet ein analytisches Modell, das die Umgehungsfähigkeit von Fuzzern mit statistischen Garantien misst. TEPHRAs Bottom-up-, grammatikgetriebene Synthese ermöglicht die Erzeugung vielfältiger Hindernisse, die den Raum der Programmsemantik systematisch sondieren.

Zusätzlich umfasst unsere Arbeit eine empirische Studie mit über 37 CPU-Jahren Rechenzeit, um die Grenzen von 31 verschiedenen Fuzzing-Systemen anhand unterschiedlicher C- und C++-Hindernisse zu untersuchen.

TEPHRA wurde im Peer-Review-Verfahren angenommen und auf der International Conference on Automated Software Engineering (ASE) im November 2025 in Seoul, Südkorea, veröffentlicht, wo es mit einem Distinguished Paper Award ausgezeichnet wurde.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

https://ucsrl.de/research/tephra

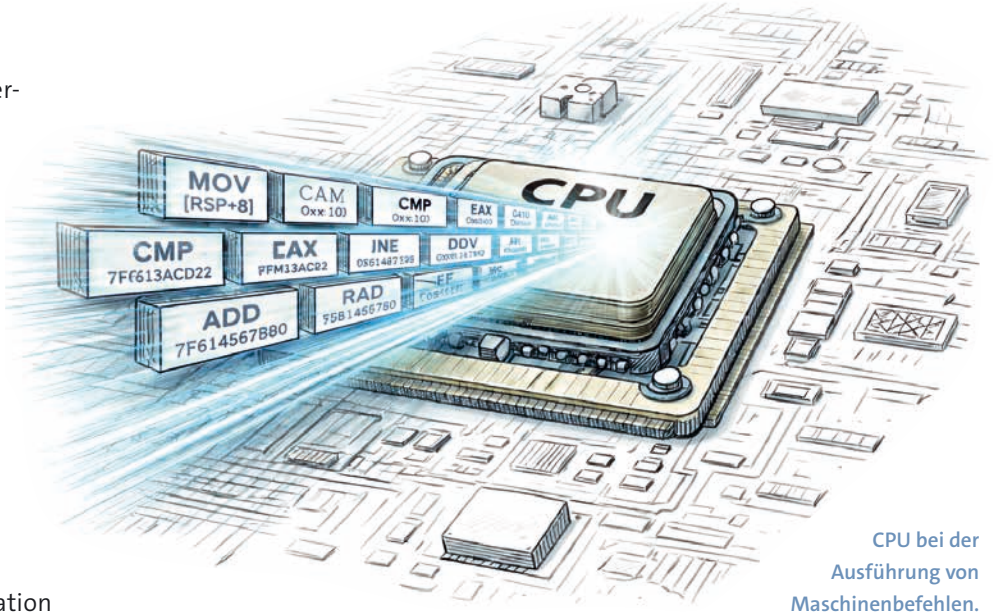
Empirische Untersuchung von Programmsemantik

Datengetriebenes Compiler-Design durch großflächige Semantikanalyse

Bei diesem Projekt wird ein großes Korpus von Systemprogrammen über verschiedene Sprachen und Architekturen hinweg analysiert, um gemeinsame semantische Merkmale zu identifizieren. Diese Merkmale erlauben Compilern, häufige Fälle effizient heuristisch zu behandeln und teure Verfahren nur bei Bedarf einzusetzen.

Ausgangslage

Allgemeine Programmiersprachen sind in der Regel Turing-vollständig. Aus wirtschaftlichen Gründen wird auch Rechenhardware (z. B. CPUs) so universell wie möglich ausgelegt. Daraus folgt, dass Sprachprozessoren wie Compiler und Interpreter zahlreiche algorithmisch schwierige und teils unentscheidbare Probleme bewältigen müssen.



CPU bei der Ausführung von Maschinenbefehlen.

So ist etwa Registerallokation NP-schwer, und der vollständige, korrekte Aufbau eines Kontrollflussgraphen für ein beliebiges Programm ist unentscheidbar. Ein korrekter Compiler muss daher für schwierige Probleme rechenintensive Algorithmen einsetzen und bei unentscheidbaren Problemen konservative Annahmen treffen.

In der Praxis verwenden Compiler jedoch schnelle Heuristiken für häufige Fälle und behalten korrekte, aber teure Verfahren als Rücksfalloption vor. Dies führt zu einer zentralen Frage für Compilerentwickler: *Was sind die häufigen Fälle?*

Kennt ein Compiler die semantischen Eigenschaften, die 80–90 % seiner Eingaben charakterisieren, kann er datengetriebene Entscheidungen treffen, statt ausschließlich auf Entwicklerintuition zu vertrauen. Zeigt sich beispielsweise, dass die meisten Eingabeprogramme strukturierten Kontrollfluss aufweisen, kann der Compiler ein einfacheres und schnelleres Verfahren zum Aufbau des Kontrollflussgraphen wählen.

Lösungsansatz

In diesem laufenden Projekt wird eine groß angelegte Untersuchung empirischer Merkmale der Semantik von Systemprogrammiersprachen durchgeführt. Dazu kompilieren wir ein sorgfältig ausgewähltes Korpus aus C-, C++-, Go-, Rust- und Ada-Programmen für x86, ARM, RISC-V, PowerPC und SPARC und analysieren verschiedene Metriken auf mehreren Abstraktionsebenen des Übersetzungsprozesses.

Prof. Dr. Stefan Brunthaler
brunthaler@unibw.de
+49 89 6004 7330
www.unibw.de/ucsrl

ABB.: S. BRUNTHALER (GENERIERT MIT KI)

Prof. Dr. Michaela Geierhos

Data Science

Das interdisziplinäre Team der Professur für Data Science vereint Kompetenzen aus den Bereichen (Wirtschafts-)Informatik und Computerlinguistik, um aktuelle und zukunftsorientierte Forschungsfragen in den Bereichen Semantische Informationsverarbeitung und Knowledge & Data Engineering zu bearbeiten.

Angewandte Forschung

Data Science ist eine interdisziplinäre, angewandte Wissenschaft. Ihr Ziel ist es, aus Daten Wissen zu generieren, um beispielsweise Entscheidungsprozesse zu unterstützen. Dabei kommen Methoden und Erkenntnisse aus Bereichen wie Statistik, Informatik und Computerlinguistik zum Einsatz.

Die Professur für Data Science erforscht Methoden zur Informationsgewinnung aus Daten und entwickelt datengetriebene Problemlösungen durch Verarbeitung, Aufbereitung, Analyse und Inferenz großer Datenmengen (Big Data). Dazu zählt unter anderem die Entwicklung von Algorithmen zur (semantischen) Textanalyse, die ihre praktische Anwendung beispielsweise im Social Media Mining findet, das wiederum zur Gefährdungserkennung von Schutzobjekten eingesetzt werden kann. Die Art der Daten ist dabei sehr vielfältig: Neben Texten werden auch Audiosignale und Bilder verarbeitet.

Praxisorientierte Lehre

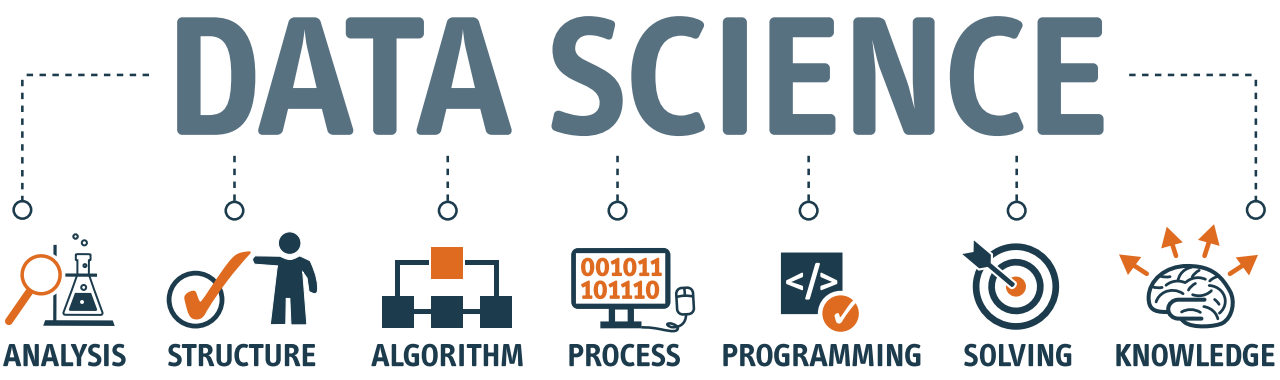
Allen Data Science-Veranstaltungen liegt ein Lehrkonzept zugrunde, das Theorie und Praxis verbindet. Die Studierenden profitieren dabei von Anfang an von der Möglichkeit, das in den Vorlesungen erworbene theoretische Wissen in abwechslungsreichen Übungen und vielfältigen praxisnahen Projekten direkt anzuwenden. Damit leistet die Professur für Data Science einen Beitrag zur exzellenten akademischen Ausbildung der Studierenden an der Universität der Bundeswehr München.

Praxisorientierte Forschung: Data Science Use Cases

Das Data Science-Team unterhält zahlreiche Kooperationen mit Partnern aus Militär, Wirtschaft und dem öffentlichen Sektor, um auch in der Forschung Theorie und Praxis miteinander zu verknüpfen. Die Anwendungsgebiete reichen derzeit vom Einsatz vertrauenswürdiger KI in polizeilichen Anwendungen über die Rekonstruktion von Audiodaten bis zur dynamischen Extraktion von nachrichtlichen Narrativen aus diversen Nachrichten-Artikeln zur Cyber-Threat-Analyse. Ein Forschungsziel beschäftigt sich mit der Identifikation und Evaluation von Kooperationspartner anhand von Patentinformationen. In diesem Jahr wurde der erste Prototyp des KiTIE-Tools verschiedenen Forschungseinrichtungen zu Testzwecken bereitgestellt. Das Feedback war sehr positiv, ebenso konnten zuvor unbekannte potentielle Partner identifiziert werden. Neben der quantitativen Evaluierung wurde auch ein qualitatives Feedback eingeholt und beides in das Tool integriert. Mit dieser verbesserten Version startet nun die zweite Testphase.

Im Verbundprojekt VIKING (Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen) wurden interdisziplinär Methoden zur Entwicklung, Bewertung und Absicherung vertrauenswürdiger KI für den polizeilichen Einsatz untersucht. Hier lag der Fokus auf erklärbaren KI-Sprachmodellen für die transparente Textklassifikation bei Sicherheitsbehörden. Hintergrund war die Herausforderung, große Textdatenmengen in der Polizeiarbeit effizient auszuwerten, ohne dabei Risiken für Individuen und Gesellschaft durch fehlerhafte oder verzerrte Modellentscheidungen in Kauf zu nehmen. Ein zentrales Ergebnis war ein System zur semantischen Modellierung von Polizeiberichten, das komplexe Inhalte strukturiert und schnell nutzbar macht. Ergänzend wurden Visualisierungen zur Bias-Bewertung, zu Debiasing-Verfahren und zu lokalen Erklärungen implementiert.

Prof. Dr. Michaela Geierhos
michaela.geierhos@unibw.de
+49 89 6004 7340
www.unibw.de/datascience



Aufgabenspektrum der Professur für Data Science.

ABB.: ADOBE STOCK / AI FARM; SHUTTERSTOCK / TRUEFFELPIX

SynData

Robuste Detektion und Analyse synthetischer Medieninhalte

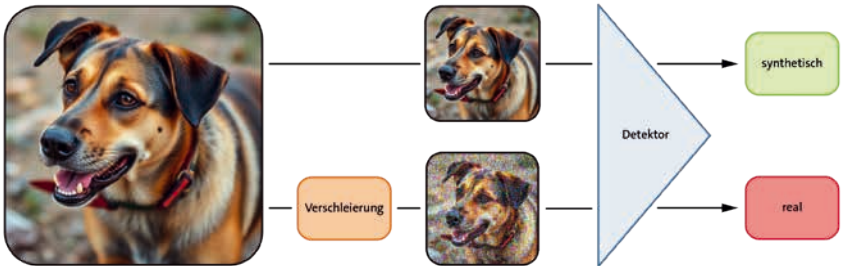
Moderne KI-basierte Programme ermöglichen Usern, in nur wenigen Klicks täuschend echte Bilddaten zu generieren. Dadurch kommt es zunehmend zu Missbrauch, etwa für Desinformation, Betrug oder andere schädliche Zwecke. Das Projekt SynData setzt hier an: Es soll dazu beitragen, den zugrundeliegenden Generierungsprozess besser zu verstehen und gleichzeitig die Erkennung künstlich erzeugter Bilddaten zuverlässiger zu machen.

Projektübersicht

Das Projekt SynData besteht aus zwei Forschungsteams mit unterschiedlichen Schwerpunkten. Ein Team untersucht Methoden zur Detektion synthetisch erzeugter Bilder, während sich das andere mit Verschleierungstechniken befasst, die generierte Bilder vor gängigen Detektionsverfahren schützen sollen. Durch diese parallele Entwicklung entstehen wertvolle Synergien. Detektoren können kontinuierlich verbessert werden, während gleichzeitig effektivere Verschleierungsmethoden entstehen, die wiederum zur Überprüfung der Robustheit der Detektoren dienen. Im Rahmen der Forschungsarbeit der letzten zwei Jahre wurden entsprechend der beschriebenen Schwerpunkte der Gruppen mehrere Lösungsansätze für die synthetische Bilddetektion und Verschleierung erarbeitet und evaluiert.

Entwicklung und Evaluierung von Detektionsmethoden

Im Bereich der Bildanalyse werden in der Regel pixelbasierte Klassifikatoren eingesetzt. Diese Modelle lernen charakteristische Artefakte synthetischer Inhalte und können dadurch zwischen realem und generiertem Bildmaterial unterscheiden. Auf dieser Grundlage sind in den letzten Jahren mehrere neue Detektionsmodelle entstanden, die den aktuellen Stand der Forschung widerspiegeln und zum Teil deutlich verbesserte Erkennungsleistungen zeigen.



Ein Detektor versucht, zwischen realen und synthetisch generierten Bildern zu unterscheiden. Verschleierungen verbergen für den Detektor relevante Merkmale, indem Pixelwerte des generierten Bildes geringfügig angepasst werden.

Entwicklung und Evaluierung von neuartigen Verschleierungsmethoden im Kontext synthetisch generierter Bilder

Die Professur für Data Science hat zunächst Grundlagenforschung zum Thema Verschleierung betrieben. Speziell wurde für das Kernthema „Sichtbarkeit von Verschleierungsartefakten“ eine umfassende Studie durchgeführt und hinsichtlich wichtiger visueller Kriterien ausgewertet. Die Resultate bilden die Grundlage für die Bewertung neuartiger Verschleierungsmethoden.

Auf Basis dieser Erkenntnisse wurde eine neuartige Verschleierungsmethode entworfen, die es ermöglicht, typische Merkmale solcher Verfahren für Betrachter weniger sichtbar zu machen. Darüber hinaus wurde eine Methode entwickelt, um die Effektivität von Verschleierungstechniken auch nach Komprimierung zu gewährleisten. Dies ist besonders relevant, da synthetische Inhalte häufig über komprimierende Webplattformen verbreitet werden. Damit rückt zugleich die Bedeutung robuster Detektionsmethoden weiter in den Vordergrund.

Die entwickelten Verschleierungsverfahren verändern synthetische Bilder derart, dass sowohl der Schutz vor Detektoren gestärkt als auch sichtbare Artefakte reduziert werden. Die im Projekt entwickelten Modelle werden genutzt, um die Robustheit der eingesetzten Detektionssysteme systematisch zu bewerten.

Amon Soares de Souza, M.Sc.
amon.soares@unibw.de
+49 89 6004 7342
https://go.unibw.de/syndata

ABB.: A. SOARES DE SOUZA / FI CODE

ADRIAN

Authority-Dependent Risk Identification and Analysis in online Networks

ADRIAN macht versteckte Gefährdungen für Web-Nutzende sichtbar: Aus öffentlich verfügbaren Daten in sozialen Netzwerken werden konsistente digitale Zwillinge erstellt. Auf dieser Grundlage quantifizieren Kennzahlen das Risiko für Identitätsdiebstahl und Spear-Phishing im Web und machen damit Gefährdungen der Privatsphäre messbar.

Online-Informationen haben Gefährdungspotenzial

Preisgegebene Informationen im Web, seien sie noch so unscheinbar, stellen in Kombination mit anderen Datenpunkten ein Gefährdungspotenzial dar. Soziale Netzwerke spielen hierbei eine Schlüsselrolle, da sie zahlreiche Inhalte bieten, die von Dritten analysiert und verknüpft werden können. Die Gefahren sind real und vielschichtig: Sie reichen von Einbrechern, die anhand sichtbarer Urlaubsfotos und Abwesenheitsmeldungen Einbrüche planen, bis hin zur Übernahme digitaler Identitäten, die zum Missbrauch von Konten und persönlichen Informationen führen kann.

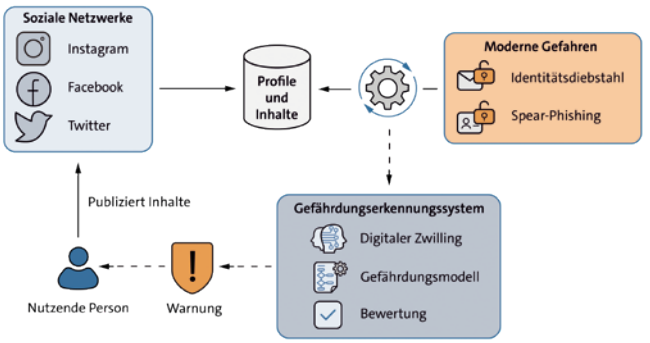
Digitale Zwillinge als Werkzeug der Gefährdungsanalyse

Die zentrale Herausforderung besteht darin, dass Nutzende sozialer Netzwerke kaum erkennen können, welche Angriffsmöglichkeiten sich durch ihren digitalen Fußabdruck eröffnen, der wissentlich und unwissentlich wächst. Einzelne Informationen wirken zwar harmlos, können in Kombination jedoch ein präzises Personenprofil ergeben. Hier setzt das Projekt an: Ziel ist es, mithilfe eines Gefährdungserkennungssystems Zusammenhänge in Datenmengen sichtbar zu machen, Risiken zu bewerten und Nutzende zu warnen, damit sie Sicherheitsmaßnahmen ergreifen können.

Da Nutzende laut Studien im Durchschnitt sieben bis acht Profile in sozialen Netzwerken unterhalten, entstehen zahlreiche verstreute Einzelinformationen, die in ihrer Gesamtheit ein umfassendes Personenprofil ergeben. ADRIAN adressiert dieses Problem mit einem Framework, das Informationen aus unterschiedlichen Profilen mittels datengetriebener Aggregationsverfahren zu konsistenten digitalen Zwillingen zusammenführt. Auf dieser Grundlage wurde ein Gefährdungsmodell entwickelt, das Methoden des maschinellen Lernens mit informationstheoretischen Konzepten kombiniert. Dies ermöglicht sowohl die Berechnung des Risikos für Identitätsdiebstahl als auch die Einschätzung der Vulnerabilität gegenüber Spear-Phishing-Angriffen. Die resultierenden Kennzahlen zeigen auf, wie attraktiv ein potenzielles Angriffsziel ist und wie einfach ein Angriff zugeschnitten werden kann.

Synthetische Inhalte bringen neue Angriffsvektoren

Vor dem Hintergrund leistungsfähiger multimodaler Modelle gewinnt zudem die Analyse synthetischer Inhalte, wie Deepfakes oder KI-generierter Social-Media-Profile, an Bedeutung. Aktuell wird untersucht, wie synthetische digitale Zwillinge generiert werden können. Diese dienen dazu, Angriffsvektoren zu analysieren und Verfahren zu entwickeln, mit denen sich reale von synthetischen digitalen Zwillingen unterscheiden lassen. Somit wird die Gefährdungsanalyse im Projekt ADRIAN um die Dimension der Erkennung und Bewertung von Fake-Inhalten ergänzt.



Vision des angestrebten Gefährdungserkennungssystems.

ABB.: DR. SERGEJ SCHULTENKÄMPER / HSBI

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

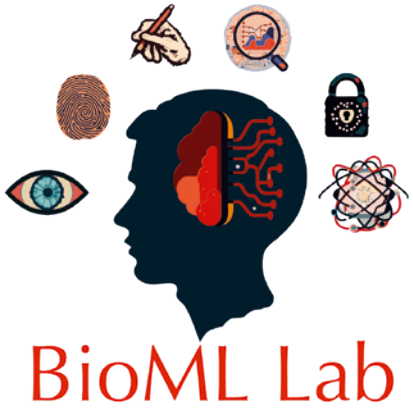
https://go.unibw.de/adrian

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

Prof. Dr. Marta Gomez-Barrero

BioML: Biometrics and Machine Learning Lab

Das BioML Lab unter der Leitung von Prof. Dr. Marta Gomez-Barrero erforscht Methoden zur Entwicklung zuverlässiger, sicherer, fairer und datenschutzfreundlicher biometrischer Erkennungssysteme. Der Schwerpunkt der Gruppe liegt auf hochinnovativer und angewandter interdisziplinärer IT-Sicherheitsforschung, basierend auf Architekturen des Machine und Deep Learning sowie auf kryptographischen Methoden.



DAS Biometrics and Machine Learning (BioML) Lab wurde im Oktober 2023 eingerichtet und ist Teil des Forschungsinstituts CODE sowie der Fakultät für Informatik. Unter der Leitung von Prof. Dr. Marta Gomez-Barrero erforscht BioML Methoden zur Entwicklung zuverlässiger, sicherer, fairer und datenschutzfreundlicher biometrischer Erkennungssysteme. Zu diesem Zweck sind Kenntnisse sowohl von Algorithmen des Machine und Deep Learnings als auch der Kryptographie erforderlich.

BioML co-organisiert und nimmt an internationalen akademischen Konferenzen wie der IEEE Int. Joint Conference on Biometrics (IJCB) und der IEEE Int. BIOSIG Conference teil. Zudem leistet BioML einen Beitrag zur European Association for Biometrics (EAB) sowie zur internationalen Normung bei ISO/IEC JTC1 SC37.

Forschungsschwerpunkte am BioML Lab

Unter biometrischer Erkennung versteht man die automatische Erkennung von Personen auf der Grundlage ihres Verhaltens und ihrer biologischen Charakteristika. Beispiele für Charakteristika, mit denen die Gruppe arbeitet, sind Gesicht, Iris, Fingerabdruck, Fingervenen, Elektrokardiogramme oder handschriftliche Unterschriften sowie Kombinationen dieser Merkmale in multibiometrischen Systemen. Neben dem Versuch, die Erkennungsgenauigkeit und die Recheneffizienz der Systeme zu erhöhen, konzentriert sich das Team auf andere wichtige Aspekte dieses Forschungsgebiets. Die Wahrung der Privatsphäre steht im Mittelpunkt, wofür biometrische Vorlagenschutzsysteme in Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO) und den einschlägigen ISO-Normen nach dem Prinzip Privacy-by-Design entwickelt werden. Darüber hinaus ist die Erkennung verschiedener Formen von Angriffen auf biometrische Systeme (z. B. Präsentationsangriffe oder Morphing-Angriffe) der Schlüssel zur Erhöhung der Sicherheit und Zuverlässigkeit der Systeme. Nicht zuletzt zielt das Team auf die Erklärbarkeit und Transparenz der Algorithmen ab, um die Akzeptanz und den Einsatz der biometrischen Erkennung zu fördern.

Aktivitäten

Im Jahr 2025 wurden die Forschungsschwerpunkte am BioML Lab weiterverfolgt: biometrischer Vorlagenschutz für datenschutzfreundliche biometrische Systeme, Erkennung von Präsentationsangriffen mit Autoencodern oder Large Vision-Language Modellen und die Analyse der biometrischen Qualität synthetischer Bilder, die mit generativen KI-Architekturen erzeugt wurden. Osman Demir stellte seine Arbeit zu Deep Hashes für den Schutz von Irisvorlagen auf der BIOSIG 2025-Konferenz in Darmstadt vor.

Die Zusammenarbeit wurde auf internationaler Ebene durch verschiedene Aktivitäten verstärkt. Gemeinsam mit Vedrana Krivokuca und Sébastien Marcel vom Idiap (Schweiz) sowie Arun Ross von der Michigan State University (USA) wurde das Springer-Handbuch „Handbook on Biometric Template Protection" fertiggestellt, das im Januar 2026 erscheint. Im April war BioML Gastgeber der 13. Ausgabe des IEEE Int. Workshop on Biometrics and Forensics (https://www.unibw.de/iwbf2025) an der UniBw München. Der Teilnehmerkreis kam aus Europa und darüber hinaus. Es gab zwei hervorragende Keynotes von Meike Ramon (Universität Lausanne) und Xiaoming Liu (Michigan State University, MSU).

Marta Gomez-Barrero leitete weiterhin den Review der ISO/IEC-Norm 30136 zum Thema „Performance testing of biometric template protection schemes", die nach der letzten Sitzung des ISO SC 37 im Juli 2025 in Singapur die DIS-Phase erreicht hat. Über die European Association for Biometrics (EAB) wurde gemeinsam mit dem US Center for Identification Technology Research (CITeR) und dem Idiap Research Institute der Martigny Biometrics Workshop organisiert. Darüber hinaus hat BioML erneut gemeinsam mit dem Fraunhofer IGD die Darmstadt Biometrics Week organisiert.

Prof. Dr. Marta Gomez-Barrero
+49 89 6004 7425
marta.gomez-barrero@unibw.de
www.unibw.de/bioml

ABB.: ADOBE STOCK / DILOK; FI CODE / MARTA GOMEZ-BARRERO

MLLMs treffen auf Biometrie

Können multimediale große Sprachmodelle dabei helfen, Angriffe auf biometrische Systeme zu erkennen?

Wir sind es mittlerweile gewohnt, Gesichtserkennungssysteme täglich zu nutzen, beispielsweise um unser Smartphone zu entsperren oder am Flughafen die Grenze zu passieren. Es handelt sich dabei in der Tat um eine bequeme und genaue Erkennungsmethode. Aber wie jedes andere IT-System sind auch diese Methoden anfällig für Angriffe – und Ziel ist es, diese zu erkennen, um eine robustere und zuverlässigere Erfahrung zu bieten.

Biometrische Präsentationsangriffe

Unter den verschiedenen Angriffspunkten biometrischer Erkennungssysteme ist der Sensor oder das Erfassungsgerät am anfälligsten: Der Angreifer benötigt kein tiefgreifendes Verständnis davon, wie die biometrische Erkennung funktioniert. Er muss lediglich ein gefälschtes biometrisches Charakteristikum herstellen, beispielsweise eine dünne Fingerabdruckauflage aus Latex oder eine 3D-Gesichtsmaske aus Silikon, um das System zu täuschen. Dabei spielt es keine Rolle, ob er sich als eine andere Person ausgeben oder einfach nur der Erkennung entgehen will – solche Angriffe werden als Präsentationsangriffe bezeichnet. Da diese eine ernsthafte Sicherheitsbedrohung für unsere Systeme darstellen, arbeitet die Biometrie-Community und das BioML Lab seit Jahren daran, Präsentationsangriffe mit zusätzlichen Modulen, den sogenannten Presentation Attack Detection (PAD)-Mechanismen, automatisch zu erkennen.

Multimedia-Großsprachmodelle (MLLMs) für PAD

In der Vergangenheit wurden entweder traditionelle Algorithmen des maschinellen Lernens wie Support Vector Machines (SVMs) auf der Grundlage von Texturmerkmalen oder in jüngerer Zeit Deep-Learning-Architekturen wie Convolutional Neural Networks (CNNs) als PAD-Module verwendet. Mit der Weiterentwicklung der Technologie tauchen jedoch immer komplexere Angriffe auf. Aber auch immer zuverlässigere Tools, um diese zu erkennen.

Gesichtsmasken können dazu genutzt werden, einen Präsentationsangriff auf biometrische Systeme durchzuführen.

Große Sprachmodelle (LLMs) wurden in erster Linie für textbasierte Anwendungen entwickelt und bereits erfolgreich für eine Vielzahl sehr unterschiedlicher Aufgaben eingesetzt. Multimodale LLMs (MLLMs) sind ihre natürliche Weiterentwicklung und können Text, Bilder und Audio verarbeiten und generieren, wodurch sie ein erhebliches Potenzial zur Verbesserung biometrischer Systeme bieten. Dieses Potenzial wurde jedoch bisher noch nicht vollständig untersucht. Wir erforschen daher, wie Large Vision-Language Modelle (LVLMs) zur Erkennung von Präsentationsangriffen in biometrischen Systemen genutzt werden können, wobei der Schwerpunkt auf ihrer Basisleistung bei Zero-Shot- und Few-Shot-Anwendungen liegt. Zu diesem Zweck wurden in den Experimenten mehrere Modelle, darunter Gemma, Qwen und Pixtral, anhand von vier verschiedenen Standard-Datenbanken für Gesichtspräsentationsangriffe analysiert und mehrere Kombinationen von System- und Benutzeraufforderungen getestet.

Die Ergebnisse sind bislang sehr vielversprechend: Die Fehlerquote liegt im ersten Benchmark unter 5 %. Andere Szenarien führen jedoch zu höheren Fehlerquoten von bis zu 23 %, und manche Angriffe sind schwieriger zu erkennen als andere. Die Fortsetzung dieser Arbeit erfolgt mit einer End-to-End-Feinabstimmung der Modelle und einer weiteren Parameteroptimierung.

Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml

ABB.: ADOBE STOCK / DREAMSTOCK (GENERIERT MIT KI)

Biometrische Daten und Datenschutz

Können wir aus einer einzigen Iris verschiedene Vorlagen generieren?

Es ist mittlerweile allgemein bekannt, dass biometrische Systeme gegenüber Authentifizierungsmethoden auf Basis von Passwörtern/Tokens eine Reihe von Vorteilen bieten: So kann man beispielsweise sein Gesicht nicht zu Hause vergessen und es nicht an eine andere Person weitergeben. Es gibt jedoch auch einige Herausforderungen: Wie können wir eine kompromittierte Irisvorlage widerrufen und eine neue erstellen? Wie oft können wir dies tun?

Was ist der Schutz biometrischer Vorlagen?

Biometrische Daten werden in der Europäischen Datenschutzgrundverordnung (DSGVO) als sensible personenbezogene Daten eingestuft. Um biometrische Systeme einsetzen und nutzen zu können, müssen die Daten daher durchgängig geschützt werden: bei der Speicherung, der Übertragung und jeder Art der Verarbeitung. Die Norm ISO/IEC 24745 definiert die Eigenschaften, die so genannte biometrische Template-Protection-Schemata (BTP) erfüllen müssen, und die Norm ISO/IEC 30136 enthält Leitlinien für die Prüfung dieser Schemata im Hinblick auf den Schutz der Privatsphäre.

Erneuerbarkeit und Unverknüpfbarkeit

Zwei der oben genannten Eigenschaften für geschützte biometrische Vorlagen sind Erneuerbarkeit und Unverknüpfbarkeit. Ersteres bezieht sich auf den Prozess der Generierung einer neuen Vorlage aus derselben biometrischen Instanz (z. B. der rechten Iris), falls die bestehende Vorlage kompromittiert wurde. Im Wesentlichen handelt es sich um denselben Prozess wie die Wahl eines neuen Passworts nach einer bekannten Sicherheitslücke.

Unverknüpfbarkeit bezieht sich in gewisser Weise auf eine sehr ähnliche Eigenschaft: Einer der Hauptvorteile der Biometrie besteht darin, dass man seine rechte Iris wiederverwenden kann, um sich in verschiedenen Systemen anzumelden, ohne deren Sicherheit zu gefährden,

Durch die Verwendung unterschiedlicher App-Parameter lassen sich aus einer einzigen Iris verschiedene, unverknüpfbare Vorlagen generieren.

im Gegensatz zu der Anforderung, unterschiedliche Passwörter für verschiedene Systeme zu haben. Damit dies funktioniert, müssen jedoch Vorlagen generiert werden, die nicht miteinander übereinstimmen, auch wenn sie von derselben rechten Iris stammen.

Wie können wir Unverknüpfbarkeit erreichen

Wir haben die Hauptfrage noch nicht beantwortet: Wie können wir Unverknüpfbarkeit erreichen? Die meisten biometrischen Vorlagenschutzsysteme verwenden dazu eine Art Parametersatz oder Schlüssel: Durch Ändern des Schlüssels wird eine neue, nicht übereinstimmende oder unverknüpfbare Vorlage generiert. Auch hier wird ähnlich wie bei der Kompromittierung eines kryptographischen geheimen Schlüssels verfahren: Es muss ein neuer Schlüssel generiert werden. Und ebenso sind nicht alle Schlüssel oder Passwörter gleich gut.

BioML untersucht derzeit, wie sich diese Probleme auf biometrische Vorlagenschutzsysteme auf Basis von Bloom-Filtern auswirken. Diese Systeme sind so allgemein gehalten, dass sie auf verschiedene biometrische Merkmale angewendet werden können. Zu diesem Zweck wird eine größere Anzahl geschützter Datenbanken simuliert, die jeweils einen anderen Schlüssel verwenden, und die Unverknüpfbarkeit wird über alle Datenbanken hinweg mit den im Standard ISO/IEC 30136 vorgesehenen Metriken gemessen. Die ersten Experimente zeigen konstante Unverknüpfbarkeitswerte für mindestens 200 verschiedene Schlüssel.

Prof. Dr. Marta Gomez-Barrero
+49 89 6004 7425
marta.gomez-barrero@unibw.de
www.unibw.de/bioml

ABB.: ADOBE STOCK / TANYA (GENERIERT MIT KI)

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

Das Team von Wolfgang Hommel forscht unter dem Leitmotiv „Entwicklung und Betrieb sicherer vernetzter Anwendungen“ an technischen und organisatorischen Sicherheitsmaßnahmen für komplexe IT-Infrastrukturen und Kommunikationsnetze mit erhöhtem Schutzbedarf – von der Konzeption bis zum praktischen Einsatz.

DIE PROFESSUR FÜR IT-Sicherheit von Software und Daten entwickelt praxisnahe Lösungen für Security-Fragestellungen, die die operativen Randbedingungen des Betriebs komplexer IT-Infrastrukturen berücksichtigen.

Am Anfang der Forschungsarbeiten und Projekte mit Dritten steht meist eine umfassende empirische Analyse. Dabei werden beispielsweise relevante Komponenten des designierten Zielsystems in virtuellen Umgebungen detailgetreu nachgebildet oder modelliert, simuliert und anschließend auf Schwachstellen analysiert. Dieser Ansatz ermöglicht die explorative Anwendung offensiver Testverfahren und damit die qualitative und quantitative Analyse von Schwachstellen in komplexen, mehrstufigen Angriffsszenarien. Daraus werden systematisch Sicherheitsanforderungen abgeleitet, die als Grundlage für die anschließende Entwicklung und Evaluation neuer Maßnahmen dienen.

Die Konstruktion und Weiterentwicklung von IT-Sicherheitsmaßnahmen folgt einem Security-Engineering-Ansatz: (Neue) Maßnahmen werden sowohl technisch konzipiert, modelliert und simuliert als auch organisatorisch möglichst nahtlos in Design-, Einführungs- und Betriebsprozesse der vorgesehenen Anwendungsgebiete integriert. Das wesentliche Ziel ist stets die konkrete Implementierung und anschließende Evaluation – mindestens im Labor, möglichst aber auch in konkreten Pilotumgebungen oder im Idealfall durch Umsetzung in wissenschaftlich begleiteten, realen Projekten. Darüber hinaus berücksichtigt das Team auch den Faktor Mensch in der Informationssicherheit sowie ökonomische und rechtliche Randbedingungen, um ganzheitliche Sicherheitslösungen zu entwickeln.

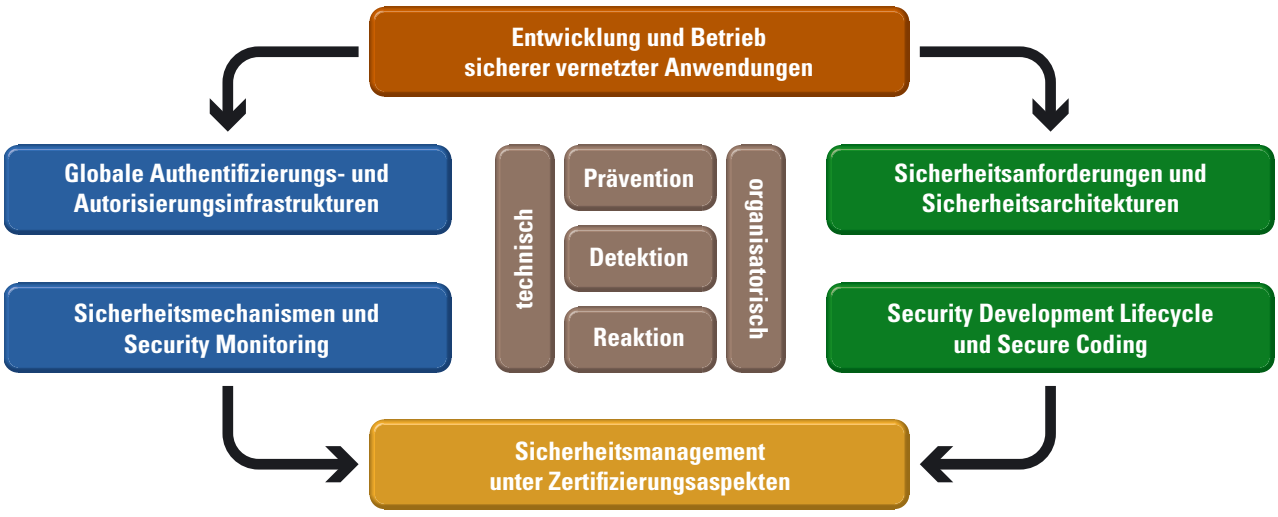
In aktuellen Forschungsvorhaben und geförderten Projekten wurde 2025 unter anderem an Quanten-Kommunikationsinfrastrukturen auf Basis von Quantum Key Distribution, Security Management für zukünftige 6G-Netze und dem sicheren Betrieb moderner Energieversorgungsnetze geforscht. Einen hohen Stellenwert nimmt auch der Praxistransfer mit Partnern aus Industrie und öffentlicher Hand ein: Beispielsweise wurde im Rahmen von dtec.bw die zweite Generation des prototypischen, Blackout-tauglichen Krisenkommunikationssystems MERLIN in Betrieb genommen; die Anwendung der dabei für zivilen Katastrophenschutz verwendeten Funktechnologie LoRa mit regelmäßigen Übungen liefert Erfahrungswerte, die sich auch auf den Einsatz in der Bundeswehr übertragen lassen.

Prof. Dr. Wolfgang Hommel

wolfgang.hommel@unibw.de

+49 89 6004 7355

www.unibw.de/software-security



Forschungsschwerpunkte der Professur für IT-Sicherheit von Software und Daten.

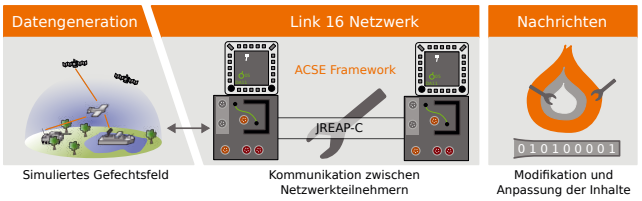
ABB.: ISTOCK / VERTIGO3D; TAUSENDBLAUWERK, QUELLE: FI CODE / W. HOMMEL

Airborne Cybersecurity Enhancement Long-Term Evolution

Taktische Datenlinks Bit für Bit unter die Lupe genommen

Taktische Datenlinks sind Kommunikationsprotokolle und -techniken, die speziell darauf ausgelegt sind, taktische Daten zwischen Einheiten auszutauschen. Diese Daten umfassen zum Beispiel Truppenbewegungen, Aufklärungsergebnisse oder auch Befehle. Ziel dieses Projektes war es, auf Bit-Ebene in den Informationsfluss einzugreifen und damit Störungen zu modellieren. Mit den Ergebnissen soll die Resilienz solcher Datenlinks verbessert werden.

MILITÄRISCHE EINHEITEN nutzen taktische Datenlinks (TDLs), um Informationen über ihren Zustand und ihre Umgebung mit anderen Einheiten zu teilen. Zum einen können sich dadurch Einheiten ein Umgebungsbild über den eigenen Wahrnehmungsbereich hinaus verschaffen, zum anderen können Führungskräfte basierend auf dem sich abzeichnenden Lagebild schneller informierte Entscheidungen über den Einsatz ihrer Kräfte treffen. Kritisch ist hierbei die korrekte der übertragenen Daten und Verarbeitung.



Skizze des Demonstrationsaufbaus.

ACSE – Die Grundidee

Jedes digitale Kommunikationssystem nutzt dedizierte Nachrichtenformate, mithilfe derer Informationen zwischen Kommunikationspartnern ausgetauscht werden. Oft arbeiten dabei mehrere Protokollschichten zusammen, um eine Ende-zu-Ende Übertragung zu gewährleisten. Gerade bei komplexen Protokollen besteht die Gefahr, dass Lücken in der Protokollspezifikation bzw. der Implementierung von gegnerischen Kräften ausgenutzt werden können. Als Gegenmaßnahme ist ausgiebiges Testen notwendig. Im Vorgängerprojekt – ACSE – wurden hierzu Test-Methodiken erarbeitet und ein entsprechendes Framework prototypisiert. Mit diesem können flexibel Nachrichtenformate sowie die Logik von Kommunikationsendpunkten nachgebildet werden und mit beliebiger Granularität modifiziert werden. Dadurch können echte Protokollimplementierungen begleitend im Entwicklungszyklus durch eine unabhängige Implementierung getestet werden. Um den Implementierungsaufwand zu senken, lag der Fokus bei der Entwicklung insbesondere darauf, Datenimporte aus existierenden maschinenlesbaren Spezifikationen zu ermöglichen.

Praktische Umsetzung für Link 16

In ACSE LTE wurden die bestehende Methodik sowie das entwickelte Framework um TDL-Unterstützung erweitert. Als Demonstrationsziel wurde Link 16 (STANAG 5516) über JREAP-C (STANAG 5518) ausgewählt, da diese Kombination von Standards innerhalb der NATO breite Anwendung findet. Dank dieser Erweiterungen konnte das Framework genutzt werden, um übertragene Daten bis auf die Bit-Ebene zu modifizieren und subtile Änderungen an logischen Inhalten vorzunehmen. Aufgrund von Abhängigkeiten innerhalb und zwischen Protokollen können schon kleinste Änderungen eine Nachricht invalidieren, da z. B. Prüfsummen nicht mehr korrekt berechnet werden. Das Framework kodiert diese Abhängigkeiten und kann, sofern gewünscht, automatisch Anpassungen vornehmen, um die syntaktische Korrektheit einer Nachricht wiederherzustellen.

Tests wurden bei Airbus DS sowohl mit synthetischen Echtzeit- als auch mit aufgezeichneten Daten in einem Airbus Integration Prototyping Lab durchgeführt. Dabei wurde auch die nahtlose Kombination mit bestehenden Testwerkzeugen (z. B. mit Link 16 Simulatoren) erprobt.

Alexander Frank
alexander.frank@unibw.de
+49 89 6004 2745
https://go.unibw.de/acse-lte

Gefördert durch: Airbus Defence und Space

ABB.: FI CODE / A. FRANK

ROLORAN

Resilienter Betrieb von LoRa-Netzen

Das dtec.bw-Projekt ROLORAN untersucht die Leistungsfähigkeit der energieeffizienten Funktechnologie LoRa („Long Range“) mit internationalen Partnern aus Militär, Behörden, Forschung und Industrie. Neben Reichweiten, Störanfälligkeit, Ortung und Mesh-Fähigkeit spielen die Angriffsdetektion und der sichere Betrieb eine ebenso große Rolle wie die Entwicklung eigener Hard- und Software für komplexe LoRa-Netze und deren Erprobung im Feld.

DIE SICHERE UND zuverlässige Kommunikation über Funkverbindungen ist unter anderem im (Military) Internet-of-Things von zentraler Bedeutung. Bei der Vernetzung vieler Sensoren und Aktuatoren in Szenarien sowohl mit als auch ohne zentrale Infrastruktur sind Störungsresistenz, Skalierbarkeit, Gewicht, Batteriebetrieb und agile Netztopologien z. B. durch Mesh- und Schwarmfähigkeit sowie einfache softwareseitige Anpassbarkeit oft essenziell, wohingegen bei Datenraten Kompromisse eingegangen werden können. Die Chirp-Spread-Spectrum-basierte Modulation LoRa stellt aufgrund hoher Reichweiten, niedriger Beschaffungs- und Betriebskosten sowie ihrer Energieeffizienz einen spannenden Lösungsbaustein für verschiedenste Anwendungen dar. Ergänzt wird LoRa durch das standardisierte LPWAN-Protokoll LoRaWAN, das über Gateways die Zusammenführung und Auswertung von Daten in einem Backend mithilfe von kommerziellen und frei verfügbaren Software-Stacks ermöglicht.

Leistungsgrenzen verschieben

Im dtec.bw-Projekt ROLORAN werden seit 2021 systematisch Hard- und Softwarekomponenten für LoRa- und LoRaWAN-Infrastrukturen erprobt und selbst entwickelt. Neben erzielbaren Reichweiten im Innen- und Außenbereich unter Berücksichtigung verschiedener Topografien werden unter anderem Aufklärung, Ortung, Jamming und Frequenzagilität untersucht, eigene LoRa-basierte Kommunikationsprotokolle u. a. für Mesh-Topologien entwickelt und kostengünstige Multi-Channel-LoRa-Radios prototypisiert. Mehrere Generationen dieser Eigenentwicklungen zeigen den mobilen und verlegefähigen Einsatz u. a. im UxV-Kontext und die Nutzbarmachung der Technologie u.a. für Datenexfiltration, Flächen- und Perimeterüberwachung sowie Blue-Force-Tracking.

Demonstrator zur Lokalisierung von LoRa-Sendern mit Routenplanung zum Standort (o. l.); Ausschnitt der Datenaufbereitung zur Sturzflutfrüherkennung (o. r.); ROLORAN-Entwicklung „LoRa Field Testing Device (LoRa FTD)“ (u. l.); Energieautarke MERLIN-Basis in Neuhaus (u. r.).

In die Praxis gebracht

Mit dem Transfer der Forschung in die Praxis als wichtigem dtec.bw-Ziel wurden in ROLORAN bereits LoRa-Installationen mit dem Österreichischen Bundesheer im Bereich Liegenschaftsmanagement und mit dem bayerischen Landkreis Bad Kissingen zum Aufbau eines Sensornetzes zur Sturzflut-Frühwarnung realisiert. 2025 wurde in der Kärntner Gemeinde Neuhaus die zweite Generation einer Blackout-tauglichen Krisen-Kommunikationsinfrastruktur auf Basis des ROLORAN Disaster Communication Protocol (RDCP) in Betrieb genommen und als Open Source veröffentlicht. Im Herbst wurde ein Prototyp zur Übertragung von Vitaldaten in medizinischen Anwendungen implementiert, um die Einsatzfähigkeit in besonders sensiblen Umgebungen zu zeigen. Derzeit wird an dedizierter Security-Sensorik für LoRa-basierte Netze und einer Methodik zur IT-sicheren, nahtlosen Integration von LoRa-Komponenten in bestehende Systeme, Plattformen und Infrastrukturen gearbeitet.

Mario Silaci

mario.silaci@unibw.de

+49 89 6004 2846

https://go.unibw.de/roloran

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

ABB.: UNIBW M / M. SILACI, M. GABATIN

Prof. Dr.-Ing. Mark Manulis

Privacy and Applied Cryptography Lab

Das PACY Lab, geleitet vom Inhaber der Professur für Privacy, Prof. Dr.-Ing. Mark Manulis, erforscht Technologien zur Verbesserung der Privatsphäre basierend auf modernen kryptographischen Methoden. Im Fokus stehen Design, Analyse und Entwicklung von kryptographischen Verfahren zum Schutz von Benutzern, Daten und Nachrichten, sowie deren praktischer Einsatz im Umfeld von Web, Cloud, IoT und Blockchain.

Forschungsschwerpunkte am PACY Lab

PACY Lab wurde im März 2022 eingerichtet und ist Teil des Forschungsinstituts CODE. Die Mitarbeitenden verfügen über tiefe Kenntnisse aus Kryptographie, Informatik und Mathematik, die sie für Grundlagen- und Anwendungsforschung erfolgreich einsetzen.

Die Schwerpunkte liegen in der Erforschung von Methoden und Verfahren auf dem Gebiet der **Privacy Enhancing Cryptography (PEC)** – dabei handelt es sich generell um kryptographische Verfahren mit speziellen Anforderungen an Vertraulichkeit und Privatheit.

Im Fokus des PACY Labs stehen das Design und der praktische Einsatz von diversen PEC-Verfahren, darunter erweiterte Verschlüsselungs- und Signaturverfahren sowie Protokolle. Das Team beschäftigt sich mit der Modellierung und Analyse von funktionellen Eigenschaften und Schutzzielen. Erforscht werden Zusammenhänge zwischen Verfahren/Eigenschaften, um das allgemeine Verständnis zu verbessern und neue Konstruktionswege zu finden. Das PACY Lab entwickelt neue PEC-Verfahren und nutzt diese zur Konstruktion von kryptographischen Protokollen zur Authentisierung und Zugangskontrolle, Verarbeitung von Daten und Transaktionen sowie zum Nachrichtenaustausch.

Beim Design und Implementierung von neuen PEC-Verfahren werden am PACY Lab alle gängigen mathematischen Techniken der Kryptographie eingesetzt, darunter auch Kryptographie mit elliptischen Kurven und bilinearen Abbildungen. Am PACY Lab wird zurzeit auch viel mit den Techniken der gitterbasierten Kryptographie gearbeitet, um die gewünschte kryptographische Sicherheit gegenüber von künftigen Quantenrechnern zu realisieren. Zu weiteren eingesetzten PEC-Techniken zählen Secret Sharing und Zero-Knowledge-Beweise.

PEC für Daten: Zugangskontrolle und Datenverarbeitung

Traditionelle Verschlüsselungsverfahren können Geheimhaltung gewährleisten, jedoch nicht direkt für die Verarbeitung von verschlüsselten Daten eingesetzt werden. Moderne PEC-Verfahren ermöglichen eine Vielzahl von Operationen auf verschlüsselten Daten, ohne dass diese während der Verarbeitung entschlüsselt werden müssen. Das PACY Lab arbeitet an funktionalen Verschlüsselungsverfahren, die mehr Flexibilität bei der Zugangskontrolle im Datenaustausch ermöglichen bzw. eine direkte Verarbeitung von verschlüsselten Daten in verteilten und Mehrnutzer-Anwendungen bieten. Zu den laufenden Forschungsarbeiten gehören Ansätze zur vollständig homomorphen Verschlüsselung und zur attributbasierten Verschlüsselung sowie kryptographische Protokolle, die Operationen (z. B. Suchabfragen) auf verschlüsselten Daten unterstützen, sowie deren Einsatz in verteilten Anwendungen.

PEC für Benutzer: Authentisierung und Nachrichtenaustausch

Digitale Signaturen bilden das Rückgrat moderner PKI. Damit können Benutzer sich authentisieren bzw. Ende-zu-Ende sichere Verbindungen aufbauen. Die Verifikation von PKI-basierten Signaturen gibt viele sensible Informationen preis, wie z. B. Identitäten, öffentliche Schlüssel und sämtliche Attribute. Das PACY Lab erforscht fortgeschrittene Signaturtechniken, um Authentifizierung mit Anonymität oder Unverfolgbarkeit zu kombinieren. Zu den laufenden Forschungsarbeiten gehören attributbasierte Signaturverfahren und damit zusammenhängende Konzepte für Anonymous-Credentials-Systeme. Darüber hinaus erforscht das PACY Lab Protokolle für sicheres und privates Messaging sowie zur verteilten und delegierbaren Authentifizierung, zum Beispiel in Verbindung mit dem neuen FIDO2-Standard für Web-Authentifizierung.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

ABB.: ADOBE STOCK / ANDRII YALANSKYI; FI CODE

PiQASO: Post-Quantum Cryptography as-a-Service für gemeinsame Übertragungssysteme und Infrastrukturen

Sicherer Übergang zur Post-Quanten-Kryptographie

Das PiQASO-Projekt zielt darauf ab, ein vollständig optimiertes und betriebsbereites PQC-as-a-Service-Framework bereitzustellen, das eine Suite quantensicherer kryptographischer Protokolle umfasst – darunter Schlüsselkapselung, digitale Signaturen, authentifizierten Schlüsselaustausch, Autorisierung, Identitätsmanagement und langfristigen Datenschutz. Dieses Framework soll ein vollständiges, quantenresistentes Äquivalent zu einer Public-Key-Infrastruktur (PKI) bieten, das sowohl gegen zukünftige Quantenangriffe sicher als auch praktisch für die nahtlose Integration in bestehende Übertragungssysteme und Infrastrukturen geeignet ist – ohne zusätzliche Client-Hardware. Damit wird eine quantensichere Verschlüsselung und Entschlüsselung für bestehende Systeme ermöglicht.

Das PiQASO-Projekt: ein Überblick

Das PiQASO-Projekt ist ein multinationales Konsortium aus zwei akademischen Einrichtungen und 23 Industriepartnern aus zwölf EU-Ländern. Das im Januar 2025 gestartete, auf drei Jahre angelegte Projekt zielt darauf ab, entscheidende Ergebnisse zu erzielen, die den Weg in eine sichere und widerstandsfähige digitale Zukunft im Zeitalter des Quantencomputings ebnen. Die zentrale Innovation ist das quantensichere und flexible PQC-as-a-Service-Framework von PiQASO – eine cloudbasierte Sicherheitslösung, die PQC-Operationen als bedarfsgesteuerte Dienste bereitstellt. Es integriert optimierte Implementierungen von NIST-zugelassenen Algorithmen (darunter Kyber, Dilithium), um Verschlüsselung, Authentifizierung, digitale Signaturen und Schlüsselmanagement über das gesamte Edge-to-Cloud-Kontinuum zu ermöglichen. Zu den Merkmalen gehören Krypto-Agilität, API-basierte Integration, modulare Authentifizierung mit Unterstützung klassischer und postquantensicherer Zertifikate, sichere Schlüsselbereitstellung über ein Key-Management-System sowie zertifizierbarer End-to-End-Datenschutz. Das Framework wird in Pilotanwendungen verschiedener Branchen – darunter Automobil, Finanzen, Energie, Gesundheitswesen, Luft- und Raumfahrt, Online-Medien, unbemannte Luftfahrzeuge und Transportwesen – validiert und demonstriert quantensichere Verschlüsselung, Authentifizierung und Datenschutz in realen industriellen Umgebungen.

Die Rolle des PACY Labs im PiQASO-Projekt

Als zentraler technischer Partner ist das PACY Lab an der Spezifikation und Implementierung mehrerer kryptographischer Algorithmen innerhalb des PiQASO-PQC-as-a-Service-Frameworks beteiligt. Im Besonderen arbeiten wir an quantensicheren Techniken für verschlüsselte Datenspeicherung, -übertragung und -freigabe unter Verwendung von Updatable Public Key Encryption (UPKE), um langfristige Vertraulichkeit und Privatsphäre zu gewährleisten. Wir erforschen neuartige, standardkonforme quantensichere UPKE-Designs unter Einsatz von Asynchronous Remote Key Generation (ARKG)-Techniken, die wir seit 2020 entwickeln, um skalierbaren und zukunftssicheren kryptographischen Schutz zu ermöglichen. Darüber hinaus tragen wir zu Schulungen und Kapazitätsaufbau bei, indem wir Lehrmaterialien für die PiQASO PQC Academy mitentwickeln, die das Bewusstsein und die Fachkompetenz im Bereich der Post-Quanten-Kryptographie in europäischen Industrien stärken soll.

Prof. Dr.-Ing. Mark Manulis
+49 89 6004 7365
mark.manulis@unibw.de
www.piqasoproject.eu

Gefördert durch: EU through European Cybersecurity Competence Centre, Digital Europe (Nr. 101190366)

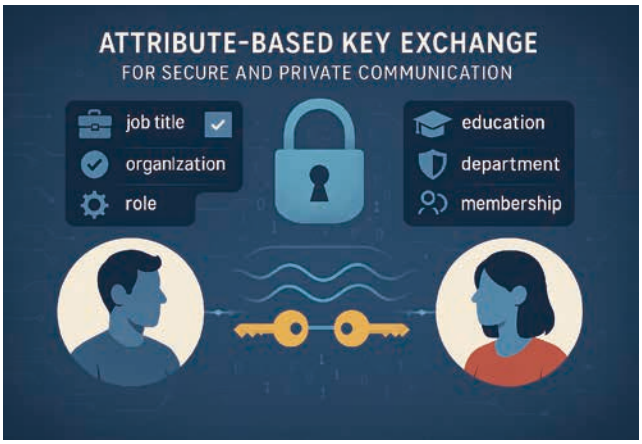
Attributbasiertes Schlüsselaustausch-verfahren mit optimaler Effizienz

Schnelle und sichere Einrichtung kryptographischer Sitzungsschlüssel auf Basis von Benutzerattributen

Der *Attribute-Based Key Exchange* (ABKE) ist ein kryptographisches Verfahren, das es Benutzern ermöglicht, einen gemeinsamen Sitzungsschlüssel zu etablieren, wenn ihre Attribute eine vordefinierte Zugriffsrichtlinie erfüllen. Dieses Verfahren erweitert klassische Schlüsselaustauschprotokolle, indem es eine fein abgestufte Zugriffskontrolle direkt in den Schlüsselaustausch integriert. ABKE findet breite Anwendung in sicheren Kommunikationssystemen – von der Client-Server-Authentifizierung bis hin zu dezentralen, rollenbasierten Netzwerken, in denen Benutzer verschlüsselte Kommunikationskanäle aushandeln können, ohne ihre Identität preiszugeben.

Herausforderungen beim attributbasierten Schlüsselaustausch

Die Entwicklung effizienter und sicherer ABKE-Protokolle bleibt eine anspruchsvolle Aufgabe. Bestehende Konstruktionen leiden oft unter hohem Rechen- und Kommunikationsaufwand, verursacht durch die Komplexität der zugrunde liegenden attributbasierten Verschlüsselung (ABE). Viele Verfahren basieren auf selektiv sicheren ABE-Schemata und ineffizienten Paarungen, was Skalierbarkeit und praktische Anwendung einschränkt. Weitere Schwachstellen bestehen in der Authentifizierung – einige Verfahren sind anfällig für Identitätsanmaßung oder bieten keine vollständige Perfect Forward Secrecy (PFS). Die zentrale Herausforderung besteht darin, ABKE-Protokolle zu entwickeln, die adaptive Sicherheit, Schutz vor Identitätsanmaßung, PFS und optimale Effizienz in Berechnung und Kommunikation vereinen.



Sicherer Schlüsselaustausch zwischen zwei Parteien basierend auf zertifizierten Attributen bzw. Rollen ohne Identitätspreisgabe.

Entwicklung schneller und sicherer ABKE-Protokolle

Das PACY Lab hat in Zusammenarbeit mit internationalen Partnern diese Herausforderungen adressiert, indem es eine neue generische und effiziente Konstruktion für Attribute-Based Key Exchange (ABKE) entwickelte, die schnelle attributbasierte Verschlüsselung (ABE) mit zweistufigen authentifizierten Schlüsselaustauschprotokollen (AKE) kombiniert. Der Ansatz baut auf aktuellen Fortschritten in der schnellen ABE-Forschung auf, insbesondere den FABEO- und FABESA-Verfahren (2024 unter Beteiligung des PACY Labs entwickelt), sowie auf effizienten AKE-Protokollen wie TOPAS und HMQV. Durch die Kombination dieser Ansätze wird adaptive Sicherheit, PFS und Schutz vor Identitätsanmaßung erreicht.

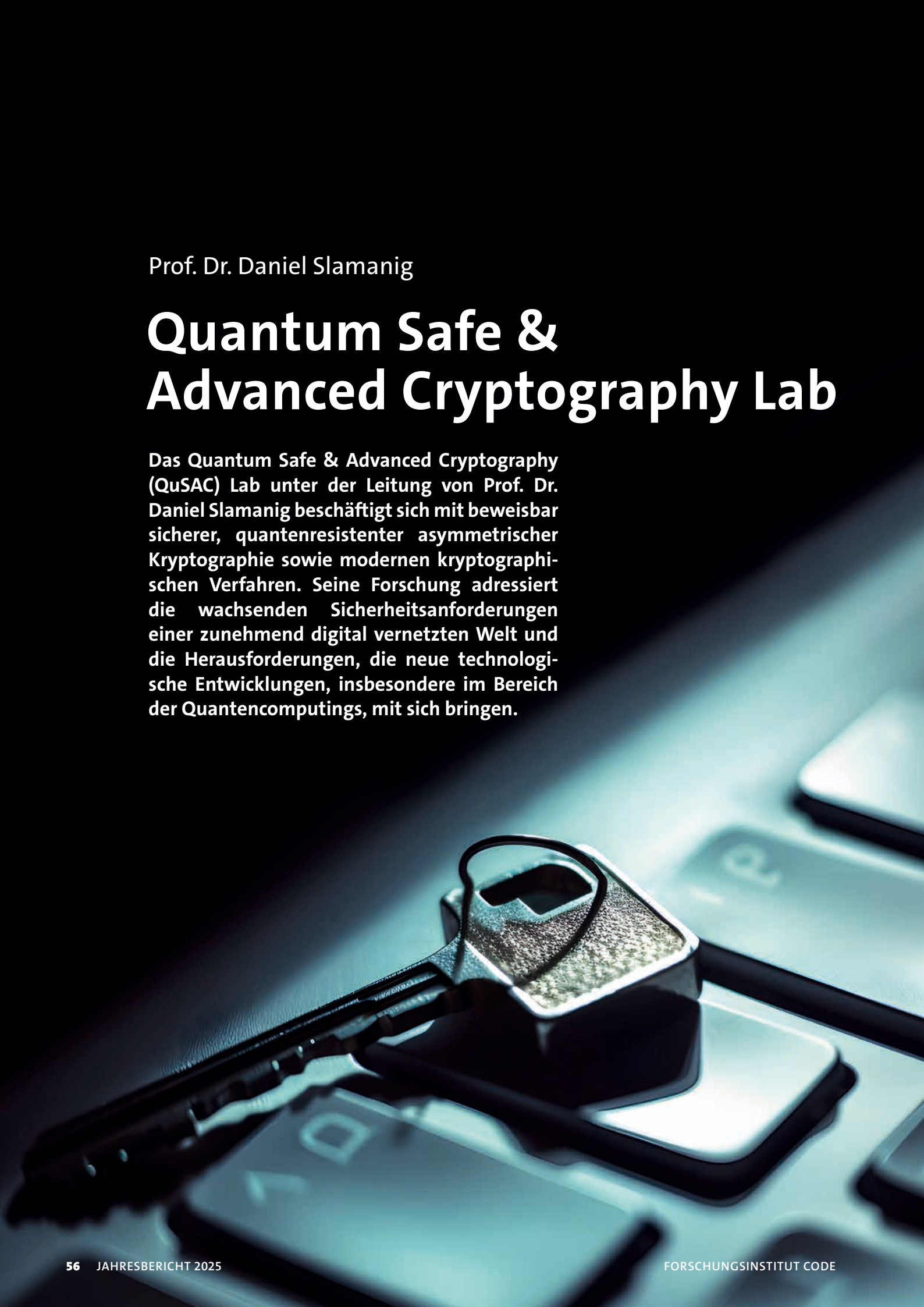
Prof. Dr.-Ing. Mark Manulis
+49 89 6004 7365
mark.manulis@unibw.de
www.unibw.de/pacy

ABB.: : GENERIERT BY DALL·E 3

Prof. Dr. Daniel Slamanig

Quantum Safe & Advanced Cryptography Lab

Das Quantum Safe & Advanced Cryptography (QuSAC) Lab unter der Leitung von Prof. Dr. Daniel Slamanig beschäftigt sich mit beweisbar sicherer, quantenresistenter asymmetrischer Kryptographie sowie modernen kryptographischen Verfahren. Seine Forschung adressiert die wachsenden Sicherheitsanforderungen einer zunehmend digital vernetzten Welt und die Herausforderungen, die neue technologische Entwicklungen, insbesondere im Bereich der Quantencomputings, mit sich bringen.



DAS QUSAC LAB FORSCHT an den theoretischen Grundlagen und praktischen Anwendungen der Kryptographie. Ein Schwerpunkt liegt auf quantenresistenter asymmetrischer Kryptographie und fortgeschrittenen kryptographischen Primitiven. Es entwickelt sowohl modulare Konzepte auf Basis generischer Bausteine als auch Verfahren, die auf konkreten mathematischen Annahmen beruhen. Beweisbare Sicherheit bildet dabei einen zentralen methodischen Leitgedanken.

Relevanz von Kryptographie

Kryptographie ist ein Kernpfeiler moderner Cybersicherheit. Sie schützt Kommunikationssysteme, digitale Identitäten und sensible Daten über verschiedenste Anwendungen hinweg. Mit der Komplexität heutiger digitaler Infrastrukturen wachsen jedoch auch die Anforderungen an Sicherheit, Effizienz und Funktionalität kryptographischer Verfahren.

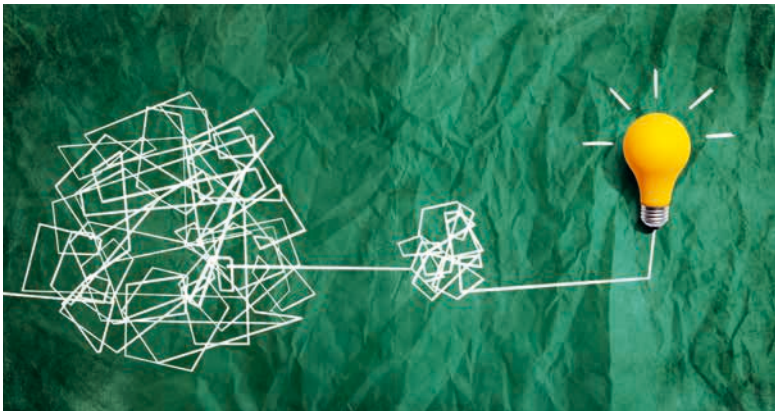
Stärkere Sicherheit – Quantencomputer und mehr

Fortschritte bei Quantencomputern gefährden viele der aktuell eingesetzten asymmetrischen Verfahren. Quantenresistente (Post-Quanten-)Kryptographie ist eine entscheidende Antwort auf diese Herausforderung. Das QuSAC Lab erforscht geeignete mathematische Problemklassen – unter anderem isogeniebasierte Kryptographie – und entwickelt darauf aufbauende Primitive. Prof. Slamanig war beispielsweise an der Entwicklung des Post-Quanten-Signaturverfahrens *Picnic* beteiligt, das im NIST-Standardisierungsprozess die dritte und finale Auswahlrunde erreichte.

Gleichzeitig reichen klassische Basisprimitive in modernen Szenarien häufig nicht mehr aus, um die erforderlichen Sicherheitsgarantien zu gewährleisten. Daher arbeitet das QuSAC-Team an fortgeschrittenen kryptographischen Konzepten mit starken Sicherheitsgarantien sowie an theoretischen Grundlagen für privatsphärefreundliche Kryptographie.

Mehr Funktionalität bei gleichzeitiger Sicherheit

Digitale Anwendungen verlangen zunehmend komplexe Funktionalitäten, die über klassische kryptographische Bausteine hinausgehen. Ein Fokus liegt auf nicht-interaktiven Zero-Knowledge-Beweisen und ihren kompakten Varianten (SNARKs), die heute in zahlreichen praktischen Systemen eingesetzt werden. Sie ermöglichen starke Sicherheitseigenschaften ohne Einbußen an Effizienz oder Skalierbarkeit.



Die Herausforderung in der Kryptographie ist das Lösen von oft paradox scheinenden Problemen.

Beitrag zur akademischen Gemeinschaft

Im Jahr 2025 wurde Prof. Slamanig eingeladen in Programmkomitees folgender internationaler Top-Konferenzen mitzuwirken: 45th International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 2026), 31st International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2025), 28th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2025), 32nd Annual ACM Conference on Computer and Communications Security (ACM CCS 2025). Darüber hinaus wurde er in die Editorial Boards des IACR Communications in Cryptology (CiC) und Proceedings on Privacy Enhancing Technologies (PoPETs) Journals eingeladen.

Entwicklung der Forschungsgruppe

Das QuSAC Lab wurde im November 2023 gegründet und umfasst derzeit drei Doktoranden und einen Post-Doc-Forscher. Die Gruppe verfügt über ein breites nationales und internationales Netzwerk, pflegt zahlreiche Kooperationen und begrüßt regelmäßig Gastwissenschaftler aus dem Ausland.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

www.unibw.de/crypto

Post-Quanten-sichere blinde Signaturen

Neue Protokolle von kryptographischen Gruppenwirkungen

Blinde Signaturen sind digitale Signaturen, bei denen die signierende Partei eine Signatur auf einer Nachricht ausstellt, ohne deren Inhalt zu erfahren. Sie sind ein grundlegender Baustein für Anwendungen, die sowohl Privatsphäre als auch Kontrolle über die Anzahl zulässiger Operationen benötigen, etwa E-Cash oder E-Voting. Ein Beispiel ist eine Bürgerin, deren elektronische Stimme vom Staat validiert werden muss, ohne dass ihre Wahl offengelegt wird, aber dennoch sichergestellt bleibt, dass sie nur einmal abstimmen kann. Blinde Signaturen ermöglichen genau dieses Gleichgewicht zwischen Anonymität und Einmaligkeit.

AKTUELLE ARBEITEN schlagen Post-Quantum Blinde Signaturen überwiegend basierend auf Gitterannahmen vor. Um jedoch eine Vielfalt kryptographischer Sicherheitsannahmen zu gewährleisten sowie Effizienz und Robustheit zu verbessern, werden alternative Ansätze benötigt, die nicht auf Gittern beruhen und ineffiziente Zero-Knowledge-Beweise vermeiden. Gleichzeitig müssen alle Sicherheitsanforderungen – insbesondere „Blindness“ und „One-More-Unforgeability“ – auch bei gleichzeitig ablaufenden Signatursitzungen erhalten bleiben.

Kryptographische Gruppenwirkingen

Gruppenwirkingen (engl. Group Actions) verallgemeinern das diskrete Logarithmusproblem auf Strukturen, für die keine effizienten Quantenangriffe bekannt sind. Gegeben ein Element x und die Wirkung $g \star x$ eines (geheimen) Gruppenelements g auf x, besteht das Group Action Inversion Problem (GAIP) darin, g zu finden. Group Actions können etwa mit Isogenien instanziiert werden (z. B. CSIDH, CSI-FiSh oder jüngst PEGASIS), aber auch – in nichtkommutativen Settings – mit linearen Codes (z. B. LESS).

Illustration von blinden Signaturen: Eine signierende Person unterzeichnet eine Nachricht, deren Inhalt sie nicht kennt.

Das Tanuki Framework

In „Tanuki: New Frameworks for (Concurrently Secure) Blind Signatures from Post-Quantum Group Actions“ (publiziert auf der ASIACRYPT 2025) wurden neue Drei-Schritt-Protokolle für Blinde Signaturen vorgestellt, die auf Group Actions basieren. Die zentrale Idee besteht darin, zufällige Permutationen zu nutzen, um die Commitments des Signierenden blind zu machen, welche aus einem Fixed-Weight-Hash der Challenges abgeleitet werden – einem Hash also, dessen Ausgabe stets dieselbe Anzahl an Nullen und Einsen besitzt. Die Technik erweitert sich auf Multi-Key-Szenarien und verhindert bekannte nebenläufige Angriffe. Die Frameworks erlauben Instanziierungen sowohl mit Isogenien (CSIDH/CSI-FiSh) als auch mit Codes (LESS) und erreichen kompakte Signaturen (z. B. ~4,5 KB für CSIDH und ~64,7 KB für LESS bei 128-Bit-Sicherheit in der nebenläufig sicheren Variante). Ein wesentlicher Vorteil besteht darin, dass diese Protokolle keine Kommutativität der Group Action erfordern und somit ein breites Spektrum post-quanten-sicherer Annahmen abdecken.

Nächste Schritte

In Zusammenarbeit mit der Norwegian University of Science and Technology (NTNU) und dem CISPA Helmholtz Center for Information Security untersucht das QuSAC-Team zudem neue Konstruktionen gitterbasierter Verfahren für Blinde Signaturen. Ziel ist es, Signaturen zu entwickeln, deren Struktur und Verifikationsschnittstelle denen konventioneller Signaturschemata entsprechen.

Prof. Dr. Daniel Slamanig
daniel.slamanig@unibw.de
+49 89 6004 7430

ABB.: SHUTTERSTOCK / APRINT

SPRINT: Neue Signaturen und Beweissystem

Neue Isogeny Proofs of Knowledge und Signaturen

Da Quantencomputer immer leistungsfähiger werden, könnten viele der heutigen kryptographischen Systeme geknackt werden. Forscher arbeiten mit Hochdruck an der Entwicklung einer Post-Quanten-Kryptographie, also Systemen, die auch gegen Quantenangriffe sicher sind. Ein vielversprechender Ansatz sind Isogenien, spezielle mathematische Abbildungen zwischen elliptischen Kurven. Isogenie-basierte Signaturschemata wie SQIsign und PRISM sind attraktiv, da sie sehr kleine Schlüssel und Signaturen erzeugen und sich daher gut für die zukünftige Post-Quanten-Sicherheit eignen.

ALLERDINGS HABEN diese Systeme auch einige Nachteile. Viele von ihnen basieren auf weniger etablierten oder sehr komplexen Sicherheitsannahmen, was es für die Community schwieriger macht, Vertrauen zu gewinnen. Einige erfordern spezielle mathematische Konfigurationen oder basieren auf Kurven mit bekannter interner Struktur, was ihre Einsatzmöglichkeiten in verschiedenen Kontexten einschränkt. Andere benötigen komplizierte Protokolle, um die Sicherheit zu gewährleisten, was sie verlangsamen oder ihre korrekte Implementierung erschweren kann. Aufgrund dieser Probleme suchen Forscher weiterhin nach isogeniebasierten Signatursystemen, die sowohl einfach zu vertrauen als auch praktisch anzuwenden sind.

Die SPRINT Signaturfamilie

Aktuelle Forschung der QuSAC-Gruppe zielt darauf ab, diese Probleme zu lösen. Sie hat eine neue Familie sehr effizienter digitaler Signaturschemata entwickelt, die auf bestehenden post-quantum Polynomial Commitment Schemes aufbauen – einer Klasse von kryptographischen Primitiven, die als Bausteine verwendet werden, um große Berechnungen schnell und sicher zu verifizieren. Durch die Kombination dieser Commitments mit neuen Techniken zu Beweisen von Isogenien hat das

SPRINT bietet sehr effiziente Beweise für die Kenntnis von Isogenien und eine Familie von Signaturschemata.

Team Signaturschemata geschaffen, deren Signaturen nicht nur schnell zu generieren und zu verifizieren sind, sondern auch auf fundierten mathematischen Annahmen beruhen.

Das Ergebnis ist eine flexible Familie von Post-Quanten-Signaturschemata, die eine vergleichbare Leistung wie die derzeit fortschrittlichsten isogeniebasierten Signaturen erzielen. Obwohl die Signaturen selbst etwas größer sind, machen die Effizienzgewinne und die soliden Sicherheitsgarantien diese Schemata zu einem überzeugenden Ansatz für zukünftige kryptographische Standards und Anwendungen. Darüber hinaus wirken sich Verbesserungen der Effizienz von Polynomial Commitment Schemes unmittelbar auf die Effizienz unserer Signaturen aus.

Zero-Knowledge Beweise für Isogenien

SPRINT dient neben Post-Quantum-Signaturen auch als Zero-Knowledge-Beweis für die Kenntnis von Isogenien: Man kann nachweisen, eine Isogenie zu kennen, ohne sie offenzulegen. Solche Nachweise sind zentral für viele Post-Quanten-sichere Protokolle, waren bisher aber oft langsam oder basierten auf speziellen Annahmen. SPRINT überwindet diese Einschränkungen, indem es moderne Polynomial-Commitment-Techniken nutzt und damit deutlich schnellere, leicht verifizierbare Beweise auf etablierten Sicherheitsannahmen ermöglicht. Dadurch schafft es eine solide Grundlage für weitere isogeniebasierte Kryptographie und zukünftige Post-Quanten-Systeme.

Prof. Dr. Daniel Slamanig
daniel.slamanig@unibw.de
+49 89 6004 7430
www.unibw.de/crypto

ABB.: SHUTTERSTOCK / JACKIE NAAM

Prof. Dr. Arno Wacker

Datenschutz und Compliance

Datenschutz und IT-Sicherheit nicht nur lehren, sondern auch leben!

EINES DER WICHTIGSTEN ZIELE der Professur ist es, Datenschutz und IT-Sicherheit nicht nur zu erforschen und zu lehren, sondern auch im Alltag zu leben. Nur so können diese Themen den Studierenden überzeugend und authentisch vermittelt werden. Darüber hinaus soll auch der breiten Öffentlichkeit gezeigt werden, dass datenschutzfördernde Technologien in den Alltag integriert werden können, sowohl im privaten als auch im geschäftlichen Bereich.

Lehre

Die Lehre der Professur gliedert sich in die Bereiche Datenschutz, Privacy Enhancing Technologies, Pentesting, Kryptologie sowie Sichere Netze und Protokolle. Datenschutz und Privacy Enhancing Technologies vermitteln den Studierenden unter anderem, was Privacy ist und warum sie sowohl für den Einzelnen als auch für demokratische Gesellschaften von Bedeutung ist. Pentesting behandelt das Testen einzelner Systeme, komplexerer IT-Dienste und ganzer IT-Infrastrukturen sowie praxisrelevante Angriffsvektoren auf Grundlage etablierter Best-Practice-Dokumentationen. Kryptologie vermittelt Grundlagen der Kryptographie sowie Kenntnisse über die verschiedenen Verfahren zur sicheren Datenübertragung in modernen Kommunikationsnetzen.

Forschung

Ein zentraler Schwerpunkt der Professur liegt auf Methoden und Mechanismen zur Unterstützung der Privatsphäre und des Datenschutzes und gliedert sich in drei verschiedene Forschungsschwerpunkte:

- Privatheitsunterstützende Mechanismen zielen auf die Stärkung der Privatheit des Einzelnen sowie auf die Erforschung von Kommunikationsregeln für das Internetzeitalter.

- Die Erhöhung des IT-Sicherheitsbewusstseins (Awareness) befasst sich unter anderem mit dem Bereich Selbstdatenschutz. Dazu entwickelt und erforscht die Professur u. a. Verfahren und Werkzeuge zur Erhöhung des Sicherheitsbewusstseins bei der Entwicklung von Softwarewerkzeugen bzw. im Umgang mit diesen.

Digitale Sicherheit und Datenschutz sind Kernbereiche von Forschung und Lehre der Professur.

- Die Kryptoanalyse klassischer Chiffren untersucht das Gebiet klassischer Verschlüsselungsverfahren mit Hilfe moderner (meta-)heuristischer Verfahren. Dabei werden unter anderem die Effizienz der Analysen sowie die Sicherheit der Algorithmen untersucht.

Wissenstransfer

Ein besonderes Anliegen der Professur ist es, interessierte Bürgerinnen und Bürger in Fragen der IT-Sicherheit zu schulen, aufzuklären und zu informieren. Dieses Ziel verfolgt das ganze Team mit Vorträgen und Workshops, die sich beispielsweise mit Pentesting, sicherem E-Mail-Verkehr im Alltag und dem Aufspüren von Sicherheitslücken beschäftigen.

Prof. Dr. Arno Wacker
arno.wacker@unibw.de
+49 89 6004 7325
www.unibw.de/datcom

ABB.: ISTOCK / MATEJMO; ADOBE STOCK

Abgelaufene Domänen in Verbindung mit E-Mail-Infrastruktur

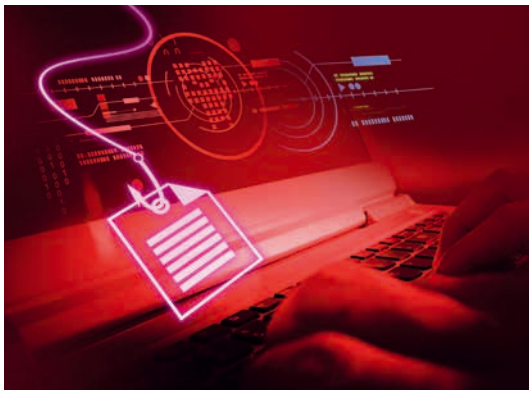
Eine empirische Studie zu abgelaufenen Domänen, welche in der E-Mail-Infrastruktur eingesetzt wurden

Dieses Forschungsprojekt behandelt eine empirische Studie zu abgelaufenen Verhaltens- und Änderungsmustern von abgelaufenen E-Mail-Domänen und ihre Auswirkung auf die E-Mail-Infrastruktur und Sicherheit.

ES IST MITTLERWEILE unbestreitbar, dass die E-Mail und die Infrastruktur, die ihr zugrunde liegt, ein alltäglicher Bestandteil sowohl des Privat- als auch des Berufslebens sind. Besonders im Behörden- und Geschäftsverkehr werden regelmäßig schützenswerte Daten übermittelt, die gegebenenfalls auch unter Geheimhaltungspflichten stehen. Dies gilt umso mehr, da derzeit ein technischer Wandel von traditionellen Methoden wie dem Telefax hin zu modernen elektronischen Übertragungsmethoden, wie etwa der E-Mail, stattfindet.

Die wissenschaftliche Gemeinschaft hat bereits in verschiedenen Forschungsarbeiten und Publikationen auf die Gefahren hingewiesen, die von abgelaufenen sowie neu registrierten Domains ausgehen können. Diese Problematik wurde jedoch bisher nicht empirisch untersucht. Daher liegt der Fokus dieses Forschungsprojektes auf der Durchführung einer empirischen Studie, um Datensätze zu erheben und neue Erkenntnisse zu gewinnen, die für die akademische Weiterentwicklung genutzt werden können. Dies umfasst unter anderem die Bestimmung der Prävalenz entsprechender Phänomene.

Insbesondere ist kritisch, dass neben der Ende-zu-Ende-Verschlüsselung der E-Mails keine Möglichkeiten des Schutzes vor abgelaufenen, neu registrierten E-Mail-Domänen existieren. Hierfür lässt sich die Analogie eines Postkastens heranziehen: Bei



Mails können über legale Wege an kriminelle Vereinigungen gelangen.

Auszug des Vormieters hat dieser sein Namensschild entfernt. Der Nachmieter oder ein Dritter kann jedoch, wenn auch rechtlich möglicherweise untersagt, technisch das Namensschild oder ein neues Namensschild mit dem Namen des Vormieters anbringen und würde so die für den Vormieter bestimmten Poststücke abfangen können.

Für die Studie wird auf öffentliche sowie teilweise öffentlich zugängliche Datensätze zurückgegriffen, insbesondere auf die Zonendateien der ICANN, die alle Domänen in den entsprechenden Top-Level-Domänen auflisten. Die in den Zonendateien enthaltenen Domains werden weiterverarbeitet, sodass unter anderem die Daten der zugehörigen E-Mail-Infrastrukturen (MX-Einträge) extrahiert werden. Mithilfe dieser MX-Einträge werden die betreffenden E-Mail-Server kontaktiert, und es werden Informationen aus den kryptographischen Zertifikaten extrahiert. Dies soll es ermöglichen, zu erkennen, ob sich ein E-Mail-Server geändert hat, etwa wenn sich der Fingerabdruck eines Zertifikats geändert hat. Allerdings lässt sich auf diese Weise nicht feststellen, ob eine Änderung bösartiger oder gutartiger Natur ist.

Insbesondere könnten die gewonnenen Erkenntnisse zur Implementierung von Sicherheitsmechanismen oder Erweiterungen der Standards genutzt werden, um die Gefahr von abgelaufenen E-Mail-Domänen zu lindern.

Linus Laurenz
linus.laurenz@unibw.de
+49 89 6004-7372

ABB.: ADOBE STOCK / JANEWS094

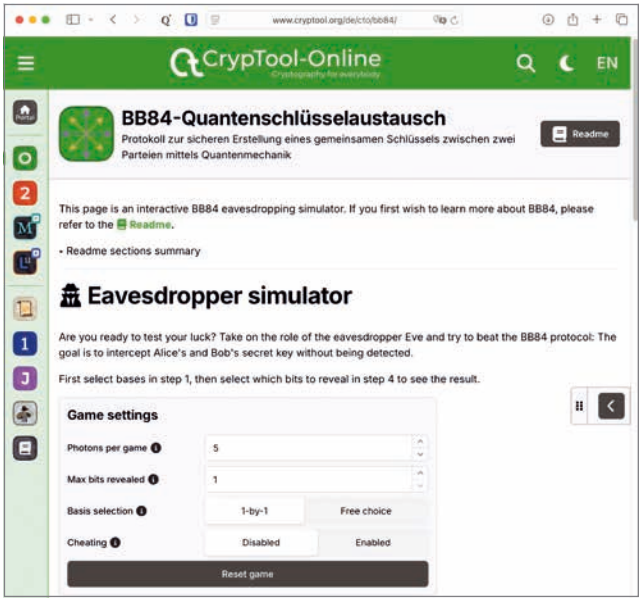
CrypTool

Weiterentwicklung der CrypTool-Website im Jahr 2025

Im Jahr 2025 wurde die CrypTool-Webseite technisch und funktional umfassend modernisiert. Der Schwerpunkt lag auf der Migration auf ein neues Webframework, der Einführung zusätzlicher interaktiver Lernanwendungen (CTO-Apps) sowie der Verbesserung von Bedienkomfort, Codequalität und Betriebssicherheit.

Neue Anwendungen und Funktionen

Mehrere Apps wurden neu integriert oder überarbeitet: Enigma, Base64, Vernam, BB84, Kyber/ML-KEM und Frequenzanalyse. Diese Projekte erforderten intensives Code-Review und teils wochenlange Nachbearbeitung, um sie auf Produktionsniveau zu bringen. Auch bestehende Module wie CryptoBrief, Monoalphabetische Substitution, Railfence/Redefence und Caesar wurden in Funktionalität und Visualisierung verbessert. Die Python-Integration erhielt einen isolierten Ausführungskontext und einen neuen Editor mit Ausgabefenster.



WebApp zum BB84-Protokoll.

Technische Updates

Das Frontend-Framework Next.js wurde auf Version 15 aktualisiert, Chakra UI auf Version 3 – ein aufwendiger Umstieg mit zahlreichen Anpassungen von Komponenten, Hooks und Styles. Das Design wurde vollständig überarbeitet, Schriftarten werden nun lokal über „@fontsource" bereitgestellt, Tabellen und Layouts sind responsiver, und die Startseite erhielt ein neues Konzept mit klarer Projektübersicht. Zudem wurde die Icon-Bibliothek auf FontAwesome 6 migriert.

Code-Qualität und Automatisierung

Neue Konfigurationen für Prettier und ESLint sorgen für konsistente Formatierung und automatische Code-Prüfung in der CI-Pipeline. Fehler in React-Hooks und Imports werden früh erkannt und korrigiert. Ein GitHub-Workflow übernimmt automatisiert Build, Release und Deployment über einen Webhook – ein großer Effizienzgewinn im Entwicklungsprozess.

Betrieb und Infrastruktur

Die Server- und Netzwerkinfrastruktur wurde konsolidiert, die Mail-Systeme vereinfacht und die Ausfallsicherheit durch doppelte Redundanz und automatische Replikation erhöht. Downloadlinks zu JavaCrypTool-Versionen werden nun beim Build zwischengespeichert, wodurch API-Ausfälle keine Fehler mehr verursachen.

Insgesamt entstand eine moderne, robuste und leicht wartbare Plattform, die technologische Basis für aktuelle und künftige kryptographische Lerninhalte bildet – mit einheitlichem Design, optimierter Performance und zukunftssicherer Architektur.

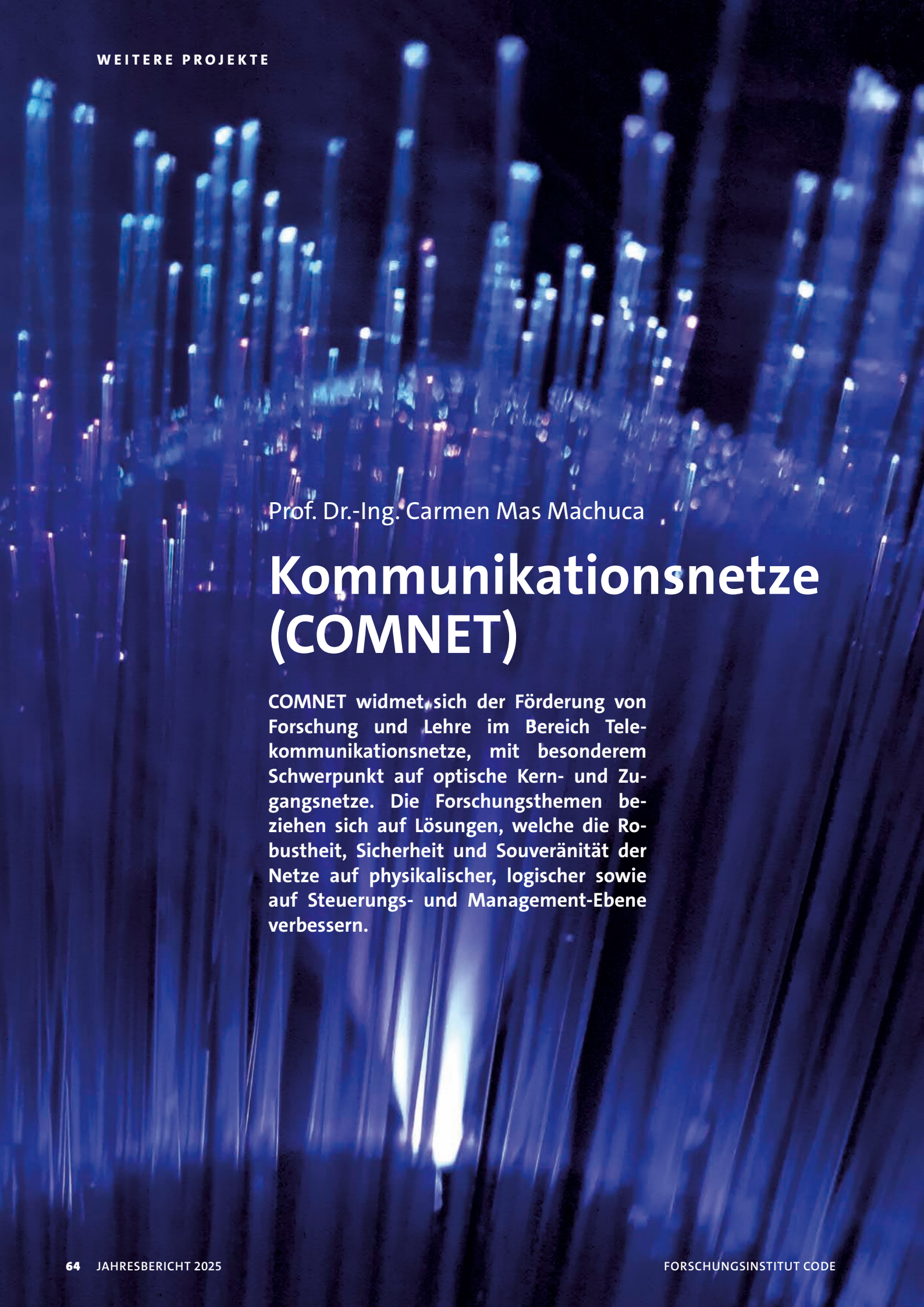
Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.cryptool.org

ABB.: CRYPTOOL / DORIS BEHRENDT



Prof. Dr.-Ing. Carmen Mas Machuca

Kommunikationsnetze (COMNET)

COMNET widmet sich der Förderung von Forschung und Lehre im Bereich Telekommunikationsnetze, mit besonderem Schwerpunkt auf optische Kern- und Zugangsnetze. Die Forschungsthemen beziehen sich auf Lösungen, welche die Robustheit, Sicherheit und Souveränität der Netze auf physikalischer, logischer sowie auf Steuerungs- und Management-Ebene verbessern.

DIE PROFESSUR FÜR KOMMUNIKATIONSNETZE wurde im April 2023 eingerichtet und ist Teil der Fakultät für Elektrotechnik und Informationstechnik an der UniBw M. Derzeit besteht das Team aus einem Postdoktoranden und zwölf Doktoranden. Insgesamt werden aktuell vier nationale BMFTR-Projekte bearbeitet, die Themen aus den Bereichen Zugangs- und Kernnetzwerke im Kontext von Resilienz, Sicherheit, Souveränität und Ressourcenzuweisung abdecken.

Forschungsthemen

Die Netzwerksouveränität gewinnt in Kommunikationsnetzen zunehmend an Bedeutung, da sie einen regulären Betrieb unabhängig von politischen, marktwirtschaftlichen oder planerischen Einschränkungen gewährleistet. Fortschritte in der Standardisierung ermöglichen die Interoperabilität von Komponenten verschiedener Hersteller und verringern so das Problem der Herstellerabhängigkeit. COMNET untersucht die optimale Anzahl von Herstellern und den Standort ihrer Komponenten, um die Netzwerksouveränität zu erhöhen. Dieser Bereich wird im Rahmen des Projekts SUSTAINET-Advance untersucht. Zusätzlich wird im BMFTR-geförderten Projekt HYPERCORE die Skalierbarkeit optischer Netze hinsichtlich Kapazität, Ausfallsicherheit und Souveränität erforscht.

Die steigende Nachfrage nach sicherer Kommunikation veranlasst Betreiber dazu, den Einsatz von QKD in ihren Netzwerken in Betracht zu ziehen. Die Forschung von COMNET befasst sich mit verschiedenen Planungsfragen mit dem Ziel, Kosten zu senken und gleichzeitig eine sichere Übertragung zu gewährleisten. Hierfür werden mehrperiodische Planungslösungen für Investitionen nach Bedarf vorgeschlagen. Darüber hinaus werden die Verteilung und Verwendung ausgetauschter Schlüssel optimiert. Diese neuen Ansätze zur Erhöhung sowohl der Sicherheit als auch der Verfügbarkeit werden derzeit in einem realen System getestet.

Zugangsnetze sind aufgrund der hohen Bereitstellungskosten das letzte Netzwerksegment, das geschützt werden muss. Daher verfügen die meisten aktuellen Zugangsnetze über eine Baumtopologie, um sich leicht an die Anzahl der angeschlossenen Nutzer anpassen zu können und die Infrastrukturkosten zu senken. COMNET modelliert, plant und bewertet verschiedene geschützte Architekturen, die die Verbindungsverfügbarkeit erhöhen können. Diese Themen werden im BMFTR-Projekt FRONT-RUNNER erforscht. Darüber hinaus werden Zuverlässigkeitsanalysen durchgeführt, um die gegenseitige Abhängigkeit zwischen Stromnetz und Kommunikationsnetzen zu bewerten und zu reduzieren, was im BMFTR-Projekt PONGO behandelt wird.

Zugangsnetze verbinden Endnutzer mit dem Kernnetz und bilden die Grundlage für den Zugang zu Kommunikationsdiensten.

Aktivitäten

Im Jahr 2025 war COMNET als Co-Vorsitzender des technischen Programmkomitees an der Organisation der internationalen Konferenz „Optical Network Design and Modelling“ (ONDM) beteiligt und hielt Gastvorträge auf der Optica OECC/PSC 2025 zum Thema „Towards Resilient and Secure QKD Networks” (Auf dem Weg zu widerstandsfähigen und sicheren QKD-Netzwerken) sowie auf der WueWoWas 2025 zum Thema „Resilience and Sovereignty Metrics and Models” (Metriken und Modelle für Widerstandsfähigkeit und Souveränität). Mehrere technische Vorträge wurden bei verschiedenen nationalen und internationalen Konferenzen eingereicht und angenommen, darunter die VDE ITG-Konferenz über photonische Netzwerke, der IEEE EuCNC & 6G Summit, die IEEE RNDM 2025, die Berlin 6G Conference, die IEEE ICTON 2025, die WueWoWas 2025 und die IEEE FNFW 2025. Einige dieser Vorträge wurden als beste Beiträge ausgezeichnet, darunter „Routing, Band, Modulation, and Spectrum Assignment with Dedicated Protection in Multiband-Elastic Optical Networks” von Dr.-Ing. Anjali Sharma auf der IEEE ONDM 2025 und „Investigating the Correlation Between Minimal Cut Set and Flow Availabilities” von Shakthivelu Janardhanan auf der WueWoWas 2025. Das COMNET-Team hat außerdem seine Arbeiten auf dem IEEE EuCNC & 6G Summit, der Berlin 6G Conference und dem IEEE ICTON präsentiert.

Prof. Dr.-Ing. Carmen Mas Machuca

cmas@unibw.de

+49 89 6004 7560

www.unibw.de/comnet

ABB.: ADOBE STOCK/ BLEDI, EIMANTAS BUZAS

Juniorprof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

Juniorprof. Molls Forschung konzentriert sich zum einen auf Reinforcement Learning, wobei ihn besonders die Kombinationsmöglichkeiten mit klassischem Operations Research sowie die Anwendungsmöglichkeiten im Prescriptive Analytics und Prescriptive Intelligence interessieren. Zum anderen forscht er an den Schnittstellen von Quantum Computing zu Optimierung und Machine Learning.

Datenbasiertes Monitoring Landsysteme

Ersatzteilprognose für das Waffensystem GTK Boxer

Das Projekt unterstützt die Einsatzbereitschaft der Bundeswehr-Landsysteme: Zur Prognose des Ersatzteilverbrauchs während Instandhaltungsmaßnahmen werden kombinierte und bereinigte Daten des GTK Boxer aus verschiedenen Datenquellen herangezogen. Das Ergebnis sind automatisierte Ersatzteilpakete sowie Visualisierungen mit klaren Kennzahlen. Diese stehen Entscheidungsträgern zukünftig auf der pCloudBw zur Verfügung.

DIE MATERIELLE Einsatzbereitschaft ist ein zentrales Anliegen der Bundeswehr. Die wachsende Menge an telemetrischen, logistischen und nutzungsbezogenen Daten eröffnet neue Möglichkeiten, den Zustand von Landsystemen frühzeitig zu bewerten und Ersatzteile gezielt bereitzustellen. Im vorliegenden Projekt soll deswegen die Methodik zum datenbasierten Monitoring von Landsystemen weiterentwickelt werden. Neben der Untersuchung der Sensorik in weiteren Teilprojekten, sollen insbesondere die bereits erhobenen Daten zu Nutzungsprofilen und Ersatzteilverbräuchen aus verschiedenen Datenquellen aggregiert und für den GTK Boxer ausgewertet werden. Somit hat das Projekt nicht nur direkte Bedeutung für die Verantwortlichen in der Bundeswehr, sondern bietet auch wissenschaftliches Innovationspotential in der Ersatzteilprognose.

Herausforderung: Datenbasis

Die vorhandenen Verbrauchsdaten enthalten zahlreiche Attribute, in denen Beschreibungen individuell formuliert wurden. Diese variierenden Bezeichnungen führen zu Inkonsistenzen, die zunächst durch eine umfassende Bereinigung behoben werden müssen. Im weiteren Projektverlauf werden die bereinigten Bestandsdaten anschließend mit Einsatz- und Sensorikinformationen fusioniert.

Innenansicht GTK Boxer.

Fortschrittliche Ersatzteilprognose

Das Projekt gliedert sich in zwei Kernsäulen. Zum einen werden neuartige Ansätze in der Ersatzteilprognose entwickelt. Dabei unterscheidet das Projekt zwischen planbaren Austauschintervallen und ungeplanten Schadensereignissen. Für den ersten Fall wird ein Verfahren entwickelt, mit dem passende Ersatzpakete identifiziert und deren Lieferfristen optimal aufeinander abgestimmt werden können. Im zweiten Fall fließen detaillierte Nutzungsprofile – etwa Fahrstrecken, Terrain-Charakteristika und Belastungsgrade – in ein Lernmodell ein, das die Wahrscheinlichkeit zukünftiger Defekte prognostiziert.

Operationalisierung und visuelle Entscheidungsunterstützung

Zweitens sollen diese Ergebnisse nicht nur theoretisch bleiben, sondern praktisch nutzbar gemacht werden. Hierzu werden die Modelle so aufbereitet, dass sie sich nahtlos in automatisierte Datenpipelines integrieren lassen. Das Projekt ist damit eines der ersten, das die neue pCloudBw-Infrastruktur der Bundeswehr für solche Anwendungen nutzt und das Projekt Prognosefähigkeit für Großgeräte der Bundeswehr aus dem Clusterprogramm Analytics und Simulation um wesentliche Funktionalitäten ergänzt. Parallel dazu wird die visuelle Entscheidungsunterstützung weiterentwickelt: In einer Weboberfläche erhalten Verantwortliche aus Beschaffung, Instandhaltung und Einsatzplanung übersichtliche Kennzahlen. So können Entscheidungen datenbasiert, transparent und zeitnah getroffen werden.

Juniorprof. Dr. Maximilian Moll

maximilian.moll@unibw.de

+49 89 6004 2248

www.unibw.de/comtessa

ABB.: ADOBE STOCK / TIERNEY; BUNDESWEHR / MANDT

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

Die Artificial Intelligence and Machine Learning (AIML) Group unter der Leitung von Prof. Dr. Eirini Ntoutsi entwickelt KI-Systeme, die technisch robust sind – also widerstandsfähig gegenüber realen Datenherausforderungen wie Bias, Datenungleichgewicht, Verteilungsverschiebungen und adversarialen Angriffen – und zugleich *gesellschaftlich verantwortungsvoll*, mit Fokus auf Fairness, Erklärbarkeit und Nachvollziehbarkeit von KI-gestützten Entscheidungen.

DZdA – Deutsches Zentrum für Digitale Aufgaben in der Hochschullehre

Generative KI-gestützte digitale Aufgabenerstellung und -bewertung zur Verbesserung von Lernergebnissen in der Hochschullehre

Das Projekt etabliert das Deutsche Zentrum für Digitale Aufgaben in der Hochschullehre (DZdA) zur Unterstützung der KI-basierten Erstellung, Bewertung und institutionenübergreifenden Nutzung digitaler Aufgaben. Fortschritte im Bereich generativer KI ermöglichen adaptive Prüfungsformate und neue Formen digitaler Lehr- und Lerninhalte, die Lernergebnisse durch gezielte Aufgabengenerierung, automatisierte Bewertung und personalisierte Lernempfehlungen verbessern.

Hintergrund und Motivation

Digitale Lehre und Leistungsbewertung haben sich in den letzten Jahren rasant weiterentwickelt, getrieben durch Fortschritte bei digitalen Plattformen und generativen KI-Modellen. Zwar zeigen diese Modelle in spezifischen Anwendungsfällen, etwa bei Zusammenfassungen oder der Feedback-Unterstützung, hohe Leistungsfähigkeit, ihre Qualität über Disziplinen, Aufgabentypen und Lernziele hinweg ist jedoch bislang nur unzureichend verstanden. Dies wirft Fragen zur Zuverlässigkeit, Konsistenz und pädagogischen Eignung auf. Zugleich sind Entwicklung und Austausch qualitativ hochwertiger digitaler Aufgaben weiterhin stark fragmentiert und institutionsspezifisch, was die Skalierbarkeit in der Hochschullehre begrenzt.

Projektvision und Ziele

Das DZdA-Projekt adressiert diese Lücke durch den Aufbau eines nationalen Zentrums für digitale Aufgaben in der Hochschullehre. Ziel ist es, die Erstellung, Bewertung und nachhaltige gemeinsame Nutzung qualitativ hochwertiger digitaler Aufgaben institutionsübergreifend zu ermöglichen. Eine strukturierte Infrastruktur und gemeinschaftsgetriebene

KI-gestützte digitale Leistungsbewertung und Lernunterstützung in der Hochschullehre.

Services sollen die Qualität der Lehre verbessern, die Wiederverwendung validierter Aufgaben fördern und skalierbare sowie adaptive Prüfungs- und Bewertungsformate über Fachdisziplinen hinweg unterstützen.

Rolle des AI & Innovation Centers

Eine zentrale Säule des DZdA ist das AI & Innovation Center unter der Leitung der AIML Group. Es entwickelt und integriert KI-basierte Methoden zur Aufgabengenerierung, automatisierten Bewertung und personalisierten Lernempfehlung. Ein besonderer Fokus liegt auf dem verantwortungsvollen und transparenten Einsatz generativer KI, um Zuverlässigkeit, Robustheit und pädagogische Angemessenheit sicherzustellen. Zudem adressiert das Center die multidimensionale Evaluation KI-generierter Aufgaben, Empfehlungen und Erklärungen für Lernende und Lehrende.

Fortschritte und Ausblick

In der initialen Projektphase liegt der Fokus auf der systematischen Evaluation generischer und bildungsspezifischer Foundation-Modelle entlang zentraler lernrelevanter Dimensionen, darunter Aufgabenqualität, Feedbackgenauigkeit, Robustheit, Ausrichtung an Lernzielen und pädagogische Eignung über verschiedene Disziplinen und Aufgabentypen hinweg. Auf dieser Basis wird ein sorgfältig ausgewähltes Modell oder ein Pool von Modellen als tragende Grundlage dienen und eine stabile Basis für die informierte und verantwortungsvolle Integration generativer KI in digitale Bewertungs- und Prüfungsworkflows schaffen.

Prof. Dr. Eirini Ntoutsi
eirini.ntoutsi@unibw.de
+49 89 6004 7420
https://go.unibw.de/dzda

Gefördert durch:
Stiftung Innovation in der Hochschullehre

Prof. Dr. Stefan Pickl

Operations Research – Forschungsgruppe COMTESSA

Die Professur für Operations Research hat in den letzten Jahren das Kompetenzzentrum COMTESSA (Core Competence Center for Operations Research, Management Intelligence Tenacity Excellence, Safety & Security ALLIANCE) begleitend entwickelt. Im wissenschaftlichen Interesse stehen die Analyse und Simulation komplexer Systeme sowie die Entwicklung von datengetriebenen Optimierungsverfahren zur IT-basierten Entscheidungsunterstützung. Seit 2023 ist Prof. Dr. Stefan Pickl ordentliches Mitglied der Deutschen Akademie der Technikwissenschaften (acatech).

REAVRS

Identifikation komplexer Angriffspotentiale für das System Bahn

Basierend auf der zunehmenden Anwendung von Digitalisierungsaspekten wie Big Data, IT etc., weist das System Bahn eine erhöhte Vulnerabilität gegenüber Angriffen von Dritten auf. Ein generelles Vorgehen bzgl. einer einheitlichen Angriffssicherheit hat sich bis dato nicht durchgesetzt. REAVRS entwickelt ein komplexes Vulnerabilitätsmodell des Systems Bahn, um anschließend intelligente (KI-basierte) Maßnahmen gegen physische- als auch Cyber-Gefahren zu entwickeln.

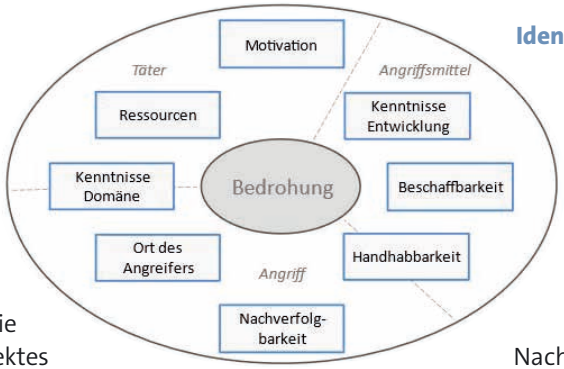
Zielsetzung

Ziel des Projekts REAVRS – einem Forschungsvorhaben vom Deutschen Zentrum für Schienenverkehrsforschung (DZSF) – ist die Charakterisierung und Analyse der aktuellen Vulnerabilität des deutschen Eisenbahnsystems. Die teilnehmenden Partner des Projektes sind die Universität der Bundeswehr München, Forschungsgruppe COMTESSA (Projektleitung) in Kooperation mit dem Forschungsinstitut CODE sowie der Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH), der CreaLab GmbH und dem Institut für Verkehrswesen, Eisenbahnbau und -betrieb (IVE) an der TU Braunschweig.

OR-basierte Systemanalyse

Der Fokus des Projekts liegt auf der Entwicklung eines komplexen Vulnerabilitätsmodells. Eine funktionale systematische Abbildung des (deutschen) Eisenbahnsystems wird entwickelt, gefolgt von einer präzisen Charakterisierung und Analyse erfolgter Angriffe sowie einer Beschreibung typischer Systemumgebungen.

Angriffsmöglichkeiten bzw. Bedrohungsszenarien werden systematisiert, und eine Gefährdungsidentifikation wird auf Basis einer OR-basierten Systemanalyse zur Risikoanalyse erstellt.



Identifikation von Kenngrößen für die Bedrohung.

Cyber-Vignetten und Angriffsszenarien

Nach Vorauswahl von Angriffspunkten werden diese zu beispielhaften Modell-Vignetten entwickelt. Damit sind Szenarien gemeint, die veranschaulichen, wie ein bestimmtes mathematisches Modell oder eine bestimmte Optimierungstechnik auf ein reales Problem angewendet wird. Bei der Systematisierung der Angriffsmittel wurden mehr als 500 physische und fast 1000 mögliche Cyberangriffe identifiziert. Eine Ursachenanalyse wird mit einer Selektion und auch Neugenerierung von repräsentativen Vignetten durchgeführt. Im finalen Schritt wird die entwickelte Methodik in eine komfortable IT-basierte Entscheidungsunterstützung Umgebung und ein zukunftsweisendes Managementcockpit eingebettet.

Identifikation von Kenngrößen

Werden die Vignetten im Detail betrachtet, so lassen sich die in der Abbildung dargestellten Kenngrößen ableiten. Sie sind die Grundlage eines zu entwickelnden Management Cockpits (Comtessa Suite).

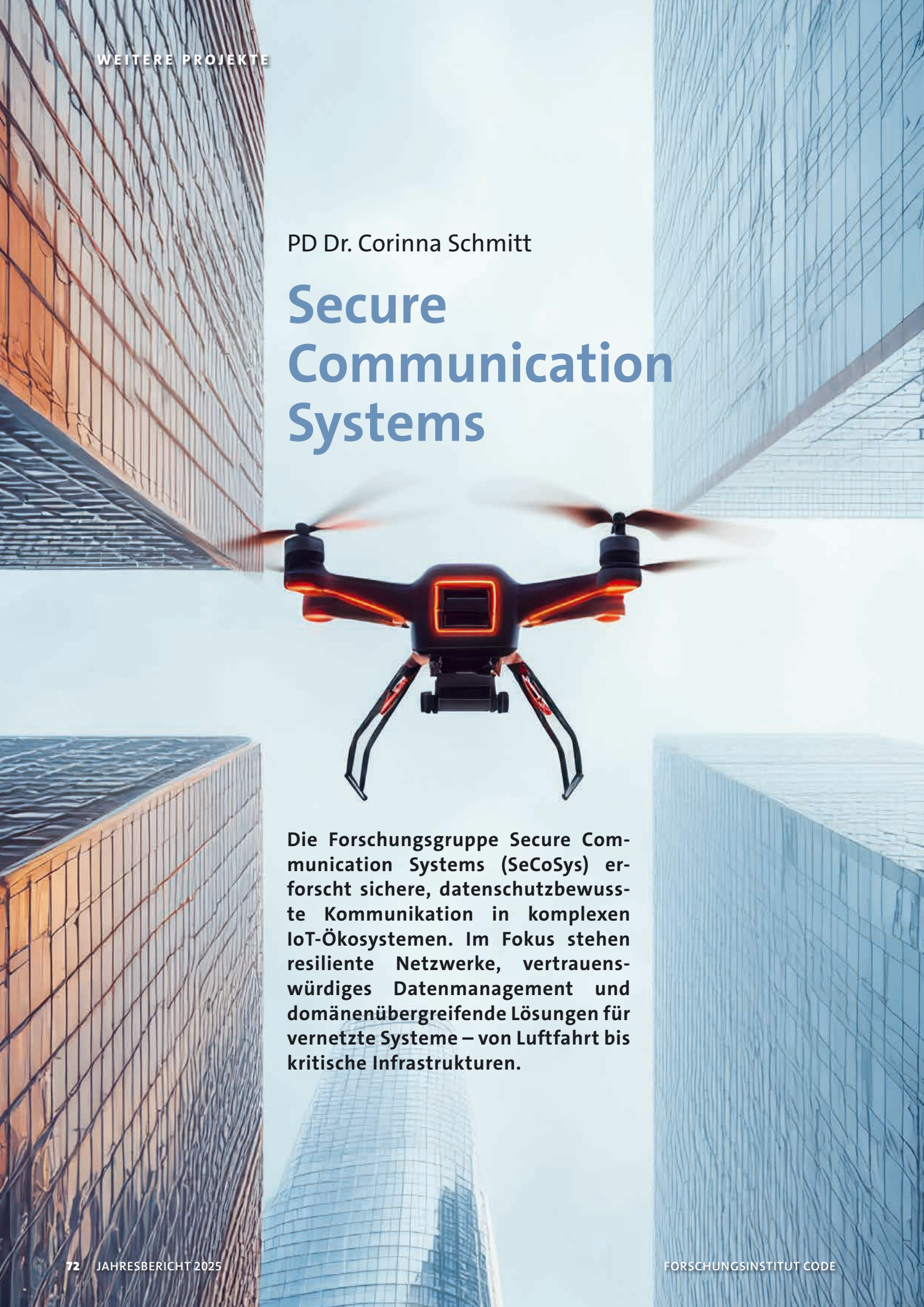
Nach der Identifikation der Kenngrößen für die Bedrohung werden die einzelnen Kenngrößen quantitativ bewertet und in eine Sicherheitsarchitektur eingebettet. Diese detaillierte Ursachenanalyse geht in die anschließende komplexe Risikoanalyse ein. Aktuell wird auch eine automatisierte Version des Bedrohungsmodells sowie ein unterstützendes Management Cockpit erarbeitet, um ein Lagebild für die Vulnerabilität des deutschen Eisenbahnsystems zu entwickeln und eine Integration des „Safety & Security“ Living-Lab am House of Logistics and Mobility (HOLM) zur Sicherheitsanalyse vorzubereiten.

Prof. Dr. Stefan Pickl
stefan.pickl@unibw.de
+49 89 6004 2400
https://go.unibw.de/reavrs

Gefördert durch: Deutsches Zentrum für Schienenverkehrsforschung (DZSF)

PD Dr. Corinna Schmitt

Secure Communication Systems



Die Forschungsgruppe Secure Communication Systems (SeCoSys) erforscht sichere, datenschutzbewusste Kommunikation in komplexen IoT-Ökosystemen. Im Fokus stehen resiliente Netzwerke, vertrauenswürdiges Datenmanagement und domänenübergreifende Lösungen für vernetzte Systeme – von Luftfahrt bis kritische Infrastrukturen.

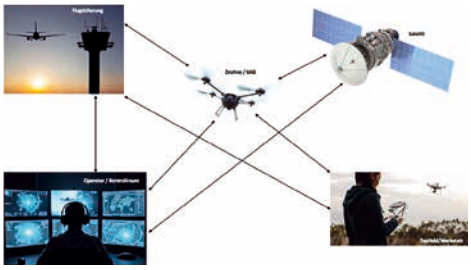
Cyber-Resilienz in der unbemannten Luftfahrt

Standardisierung von IT-Sicherheit und Resilienz für den Betrieb unbemannter Luftfahrtsysteme

Unbemannte Luftfahrtsysteme – oft „Drohnen“ genannt – gewinnen in Wirtschaft, Verwaltung und Sicherheitsorganisationen an Bedeutung. Neben klassischer Flugsicherheit sind auch digitale Risiken zentral. Die SeCoSys-Gruppe am FI CODE treibt gemeinsam mit dem UAV DACH e.V. in der Competence Group IT Safety & Security und Behörden/Industrie die Standardisierung von IT-Sicherheitsmaßnahmen für UAS voran und entwickelt praxisnahe Grundschutz-Profile zur Absicherung vernetzter Systeme.

UNBEMANNTE Luftfahrtsysteme (engl. Unmanned Aircraft System(s), UAS) kommen heute in vielfältigen Anwendungsbereichen – von logistischen Aufgaben über Katastropheneinsätze bis hin zu sicherheitskritischen Missionen bei Bundeswehr und Behörden – zum Einsatz. Dies bringt neben Anforderungen an Flug- und Betriebssicherheit auch eine erhebliche Ausweitung digitaler Angriffsflächen mit sich, da moderne UAS komplexe und zugleich vernetzte Systeme sind: Sie interagieren über Funk- und Netzwerkschnittstellen und verarbeiten Navigations- sowie Missionsdaten und sind damit potenziellen Cyberrisiken ausgesetzt. Kommt es zu Ausfällen oder Manipulationen der Firmware, den Kommunikationskanälen oder den Leitdaten, können nicht nur der Betrieb und Einsatz gestört werden, sondern auch Menschen und Sachwerte gefährdet werden.

Ziel der Forschungsgruppe Secure Communication Systems (SeCoSys) ist es, mit Hilfe von IT-Grundschutz-Profilen eine systematische und leicht umsetzbare Grundlage für die Informationssicherheit beim UAS-Betrieb zu liefern. Dabei werden etablierte Standards genutzt und praxisgerecht auf die Besonderheiten der unbemannten Luftfahrt adaptiert. In Zusammenarbeit mit der Competence Group IT Safety & Security des UAV DACH e. V., eines europäischen Verbands für unbemannte Luftfahrt, der Akteure aus Industrie, Forschung und Staat vernetzt und Rahmenbedingungen für sichere, effiziente UAS-Einsätze gestaltet, werden Profile erarbeitet, die konkrete Empfehlungen zur Absicherung von IT-Komponenten, Prozessen und Verantwortlichkeiten entlang des Lebenszyklus unbemannter Systeme liefern. Bisher wurden hierzu zwei Profile unter Mitwirkung von SeCoSys entwickelt, die auf dem etablierten IT-Grundschutz-Ansatz des Bundesamts für Sicherheit in der Informationstechnik (BSI) aufbauen:



Schematische Darstellung der Referenzarchitektur samt Kommunikationswegen.

- Band 1: IT-Grundschutz-Profil für die Betriebskategorie „Open“, das sich an UAS-Betreiber aller Art richtet und Grundanforderungen an die Informationssicherheit beim Betrieb offener, nicht-spezialisierter Systeme festlegt.
- IT-Grundschutz-Profil für den Betrieb von Uncrewed Aircraft Systems in Behörden und Organisationen mit Sicherheitsaufgaben (BOS), das ergänzende Profile für Organisationen mit Sicherheitsaufgaben enthalten, die auf dem offenen Profil aufbauen und spezifische Anforderungen berücksichtigen.

  Die Profile enthalten Referenzarchitekturen, Gefahren- und Risikoanalysen, Maßnahmenkataloge für technische und organisatorische Sicherheit sowie Hinweise zur Integration von Sicherheitsprozessen in bestehende Betriebskonzepte. Sie adressieren typische Schwachstellen wie mangelnde Absicherung von Kommunikationsschnittstellen, ungeschützte Firmware-Updates, fehlende Log- und Monitoring-Mechanismen oder unzureichende Authentifizierungsverfahren.

PD Dr. Corinna Schmitt

corinna.schmitt@unibw.de

+49 89 6004 7314

www.unibw.de/secosys

ABB.: ADOBE STOCK/ DARKIN-STUDIO; CORINNA SCHMITT; ADOBE STOCK (4)

ABB.: ADOBE STOCK / RINRADA

Kooperationen

Deutschland und die Welt

Nationale Partner

Das FI CODE arbeitet in Deutschland mit 74 Partnern in 46 Städten und Gemeinden zusammen.

DIE ZUSAMMENARBEIT mit anderen Universitäten, öffentlichen Einrichtungen und Wirtschaftsunternehmen gehört zum Selbstverständnis von CODE: Mit und von unseren Partnern lernen wir und können erste Schritte in Richtung der Umsetzung unserer Forschungsergebnisse in der Praxis gehen.

Gleichzeitig sorgt der enge Austausch dafür, dass wir die konkreten Frage- und Problemstellungen unserer Partner verstehen und aus wissenschaftlicher Perspektive betrachten können.

Innerhalb von Deutschland ist unser Netzwerk besonders eng. Als Teil der Universität der Bundeswehr München arbeiten wir bundesweit mit 74 Institutionen in 46 Städten und Gemeinden zusammen. Besondere Schwerpunkte liegen dabei auf Bayern bzw. dem Münchner Raum, Nordrhein-Westfalen und Hessen. ■

	Partner	Ort
1	Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur)	Halle (Saale)
2	Airbus Defence and Space GmbH	Taufkirchen/Manching
3	Akhetonics GmbH	Berlin
4	Bayerisches Landesamt für Sicherheit in der Informationstechnik (LSI)	Nürnberg
5	Bayerisches Landeskriminalamt (BLKA)	München
6	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)	Koblenz
7	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Bonn
8	Bundeskriminalamt (BKA)	Wiesbaden/Berlin
9	Bundessprachenamt (BSprA)	Hürth
10	BWI GmbH	Meckenheim
11	Christian-Albrechts-Universität zu Kiel (CAU)	Kiel
12	CISPA Helmholtz-Zentrum für Informationssicherheit	Saarbrücken
13	Cyber Security Operations Centre der Bundeswehr (CSOCBw)	Euskirchen
14	Deutsches Institut für Normung (DIN)	Berlin
15	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)	Köln/Oberpfaffenhofen
16	dida Datenschmiede GmbH	Berlin
17	Eberhard Karls Universität Tübingen	Tübingen
18	ESG Elektroniksystem- und Logistik-GmbH	München
19	FAST-DETECT GmbH	München
20	Forschungszentrum L3S	Hannover
21	Frankfurt University of Applied Sciences	Frankfurt a. M.
22	Fraunhofer-Institut für Digitale Medientechnologie (IDMT)	Ilmenau/Oldenburg
23	Fraunhofer-Institut für Graphische Datenverarbeitung (IGD)	Darmstadt
24	Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)	Erlangen/Nürnberg
25	Führungsakademie der Bundeswehr (FüAkBw)	Hamburg
26	Gottfried Wilhelm Leibniz Universität Hannover (LUH)	Hannover
27	GSI Helmholtz-Zentrum für Schwerionenforschung	Darmstadt
28	Helmholtz-Zentrum Dresden-Rossendorf (HZDR)	Dresden
29	Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg (HSU/UniBw H)	Hamburg
30	Hessisches Landeskriminalamt (HLKA)	Wiesbaden
31	Hessisches Polizeipräsidium für Technik (HPT)	Wiesbaden
32	Hochschule Bielefeld (HSBI)	Bielefeld
33	Hochschule Bochum	Bochum
34	Hochschule Darmstadt (h_da)	Darmstadt
35	Hochschule für Angewandte Wissenschaften Hamburg (HAW Hamburg)	Hamburg
36	Hochschule für Technik und Wirtschaft Berlin (HTW)	Berlin
37	Hochschule für Wirtschaft und Recht Berlin (HWR)	Berlin

	Partner	Ort
38	IDEMIA Identity & Security Germany AG	Bochum
39	Infineon Technologies AG	Neubiberg
40	Leibniz-Institut für Neue Materialien (INM)	Saarbrücken
41	Julius-Maximilians-Universität Würzburg (JMU)	Würzburg
42	Karlsruher Institut für Technologie (KIT)	Karlsruhe
43	Landeskriminalamt Baden-Württemberg (LKA BW)	Stuttgart
44	Landeskriminalamt Nordrhein-Westfalen (LKA NRW)	Düsseldorf
45	Landkreis Bad Kissingen	Bad Kissingen
46	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ)	Garching
47	Ludwig-Maximilians-Universität München (LMU)	München
48	Marinekommando (MarKdo)	Rostock
49	Minol-ZENNER-Gruppe	Leinfelden-Echterdingen
50	MTU Aero Engines AG	München
51	Nationales Zentrum für angewandte Cybersicherheit ATHENE	Darmstadt
52	nuix	Frankfurt a. M.
53	Ostbayerische Technische Hochschule Amberg-Weiden (OTH)	Amberg/Weiden
54	Otto-von-Guericke-Universität Magdeburg (OVGU)	Magdeburg
55	Polizeipräsidium München	München
56	RapidMiner GmbH	Dortmund
57	Rohde & Schwarz GmbH & Co. KG	München
58	Ruhr-Universität Bochum (RUB)	Bochum
59	secunet Security Networks AG	Essen
60	Siemens Energy AG	München
61	Technische Hochschule Würzburg-Schweinfurt (THWS)	Würzburg/Schweinfurt
62	Technische Universität Chemnitz	Chemnitz
63	Technische Universität Darmstadt	Darmstadt
64	Technische Universität Dresden (TUD)	Dresden
65	Technische Universität Ilmenau	Ilmenau
66	Technische Universität München (TUM)	München
67	TÜV Informationstechnik GmbH (TÜV IT)	Essen
68	Universität Konstanz	Konstanz
69	Universität Potsdam	Potsdam
70	Verein zur Förderung eines Deutschen Forschungsnetzes e. V. (DFN-Verein)	Berlin
71	VISTA Geowissenschaftliche Fernerkundung GmbH	München
72	Wehrtechnische Dienststelle für Informationstechnologie und Elektronik (WTD 81)	Greding
73	Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	München
74	Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw)	Bonn


11 Kiel
Rostock 48
3 8 14 16 36 37 70 Berlin
Hamburg 25 29 35
22 Oldenburg
20 26 Hannover
69 Potsdam
54 Magdeburg
32 Bielefeld
33 38 58 Bochum
Dortmund
59 67 Essen 56
44 Düsseldorf
Köln 15
9 Hürth
7
13 Euskirchen
Bonn 74
Meckenheim 10
Koblenz 21 6
52 Frankfurt/Main
8 30 31 36 Wiesbaden
Darmstadt 23
27 51 34 63
12 40 Saarbrücken
42 Karlsruhe
43 Stuttgart
Leinfelden-Echterdingen 49
17 Tübingen
68 Konstanz
Halle/Saale 1
22 65 Ilmenau
28 64 Dresden
62 Chemnitz
45 Bad Kissingen
Schweinfurt 61
Würzburg 41 61
Erlangen 24
Nürnberg 4
Weiden 53
Amberg 53
5 18 57 19 60 47 66 50 71 55 73
Greding 72
Manching 2
Garching 46
München
Neubiberg 39
Oberpfaffenhofen 15
Taufkirchen 2
Legende
1 Standortnummer der Partner
Standorte der Partner

Internationalität

Auch international pflegt das FI CODE ein großes Netzwerk. Im Jahr 2025 stammten die Mitarbeitenden aus 19 Ländern. In 27 Ländern gab es 79 Kooperationspartner.

Mitarbeitende

Nationalität	Anzahl
brasilianisch	1
britisch	1
bulgarisch	1
deutsch	112
französisch	2
griechisch	2
indisch	8
indonesisch	1
italienisch	4
kosovarisch	1
kroatisch	1
mexikanisch	1
niederländisch	1
österreichisch	13
polnisch	1
slowenisch	1
spanisch	3
südkoreanisch	2
ungarisch	1
Gesamt	**157**

Internationale Kooperationspartner

Land	Partner
Australien	CSIRO Data61
	Royal Melbourne Institute of Technology (RMIT)
	University of News South Wales (UNSW)
Belgien	KU Leuven
	University of Brussels (VUB)
	University of Louvain (UCL)
Dänemark	Technical University of Denmark
Estland	eu-LISA
Finnland	Tampere University
Frankreich	Air and Space Force Academy Research Center (CREA)
	ENS Lyon
	EURECOM
	Grenoble Alps University (UGA)
	IDnow

ABB.: ISTOCK / BLUE PLANET STUDIO

Land	Partner
Frankreich	National Institute for Research in Digital Science and Technology (Inria)
Griechenland	Agroknow IKE
	Athena Research and Innovation Center (ARC)
	Centre for Research and Technology Hellas (CERTH)
	EXUS Software
	University of Athens (UoA)
	Ubitech
	University of Ioannina
Italien	Abaco
	Fondazione Bruno Kessler (FBK)
	Univeristy of Bologna
	University of Genoa
	University of Roma Tre
	Univeristy of Trento
	University of Turin
Japan	Kyoto University
	National Institute of Information and Communications Technology (NICT)
	NTT Social Informatics Laboratories
Kanada	University of Waterloo
Luxemburg	University of Luxembourg
Neuseeland	University of Auckland
Niederlande	Eindhoven University of Technology (TU/e)
	University of Groningen
	University of Twente
Norwegen	Norwegian University of Science and Technology (NTUT)
	University of Oslo
	Oslo Metropolitan University (OsloMet)
Österreich	AIT Austrian Institute of Technology
	Austrian Armed Forces
	Carinthia Emergency Services
	Complexity Science Hub Vienna (CSH)
	Johannes Kepler University Linz (JKU)
	Kelag-Konzern
	Municipality of Neuhaus, Carinthia

Land	Partner
Österreich	Software Competence Center Hagenberg
	University of Applied Sciences Campus Vienna
	University of Applied Sciences Upper Austria (FH OÖ)
	Paris Lodron University of Salzburg (PLUS)
	QUS Tech
	Vienna University of Technology
Polen	Wroclaw University of Science and Technology (WUST)
Rumänien	Babeș-Bolyai University (UBB)
Schweiz	EPFL
	IBM Research Zurich
	Idiap Research Institute
	Univeristy of Lausanne
	University of St. Gallen (HSG)
Serbien	Foodscale Hub
Slowakei	Pavol Jozef Šafárik University
Spanien	Autonomous University of Madrid (UAM)
Südkorea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Tschechien	Center for Environmental and Technology Ethics
	Masaryk University (MU)
Ungarn	Eötvös Loránd University (ELTE)
USA	Auburn University, College of Engineering
	Brave Software
	Brown University
	Michigan State University
	Naval Postgraduate School (NPS)
	University of Arizona, College of Engineering
Vereinigtes Königreich	University of Birmingham
	University of Sheffield
	University of Surrey
Zypern	Centre for Social Innovation (CSI)

Forschungsbesuch aus Kroatien stärkt die Entwicklung neuer Cybersicherheitslösungen

Vom 9. bis 15. November 2025 empfing das Forschungsinstitut CODE eine Gruppe von Wissenschaftlern der Universität Zagreb und ihres Spin-off Unternehmens CyberArrange Security Solutions. Die Gäste aus Kroatien hatten die Gelegenheit, ihre Arbeit im Bereich der Automatisierung von Cybersicherheitsübungen vorzustellen und sich mit den Mitarbeitern von CODE auszutauschen.

Gäste aus Kroatien während ihrer Präsentation im FI CODE (v. l. n. r.: Dr. Ivan Kovačević, Filip Katulić, Mateo Mamut, and Dora Pavelić)

ES IST ERFREULICH, wenn Kontakte, die während Forschungsprojekten geknüpft wurden, weiter gepflegt werden können. Mehr als zwei Jahre sind seit dem ersten Forschungsbesuch von Dr. Ivan Kovačević vergangen, damals Doktorand an der Fakultät für Elektrotechnik und Informatik (FER) der Universität Zagreb. Ausgehend von seinen Forschungsinteressen und seiner Doktorarbeit gründete Dr. Kovačević 2023 das Deep-Tech-Spin-off-Unternehmen CyberArrange Security Solutions (CASS). Die enge Forschungszusammenarbeit und beratende Unterstützung durch die FER wurden erfolgreich fortgesetzt, was zu 15 Veröffentlichungen führte, die von der Forschungsgruppe auf Konferenzen und in Fachzeitschriften publiziert wurden. Aktuell erforschen FER und CASS die Anwendung von großen Sprachmodellen (LLMs) in der Ausbildung von Cybersicherheitsexperten und entwickeln Technologien, mit denen realistische Cyber-Range-Übungen automatisch vorbereitet werden können.

Da sich die Forschungsarbeiten von FER und CASS zu Cyber-Übungsplätzen, automatischer Übungsgenerierung und Cybersicherheit für kritische Infrastrukturen mit den Forschungsbereichen von FI CODE überschneiden, besteht ein gegenseitiges Interesse an der Vertiefung und Ausweitung der Zusammenarbeit. Die Erfahrung mit Cybersicherheitstrainings beim FI CODE zeigt, dass die Übungsvorbereitung ein zeitaufwändiger Prozess ist. Daher besteht Bedarf und Interesse daran, das Potenzial solcher KI-gestützten Technologien weiter zu untersuchen.

Während des einwöchigen Besuchs im November bot sich eine hervorragende Gelegenheit zum Erfahrungs- und Wissensaustausch sowie zur Durchführung von Übungen und Tests in der Cyber Range des FI CODE. Ziel des Besuchs war es, einen genaueren Einblick in die Konzeption und Durchführung von Cybersicherheitsübungen in einer solchen Umgebung zu gewinnen. Dies ist eine wertvolle Unterstützung für die Weiterentwicklung der Technologien von CASS.

Als junges Start-up-Unternehmen hat CyberArrange bereits rund 400.000 € an Fördermitteln aus wettbewerbsorientierten Zuschüssen (z. B. NextGenerationEU-Instrument) und Industriepartnerschaften erhalten, was die weitere Entwicklung und Aktivitäten des Unternehmens ermöglicht. CODE freut sich als wissenschaftlicher Partner, FER und CASS auch in Zukunft wieder begrüßen zu dürfen und sieht weiteren Kooperations- und Austauschmöglichkeiten, insbesondere im Rahmen von EU-finanzierten Projekten, erwartungsvoll entgegen.

Kontakt beim FI CODE
Ivana Buntić-Ogor
ivana.buntic-ogor@unibw.de
www.unibw.de/code/

Kontakt bei FER
Filip Katulić
filip.katulic@fer.hr
www.fer.unizg.hr/en

Kontakt bei CASS
Dr. Ivan Kovačević
info@cyberarrange.com
https://cyberarrange.com/en

ABB.: CYBERARRANGE SECURITY SOLUTIONS

Deutsch-französischer Austausch im Bereich Quantencomputing

Drei Wochen lang war Dr. Wolfgang Gehrke vom Forschungsinstitut CODE zu Gast an der französischen École de l'air et de l'espace in Salon-de-Provence. Im Mittelpunkt des Aufenthalts standen das Thema Quantencomputing sowie der Aufbau und die Vertiefung gemeinsamer Lehr- und Kooperationsformate zwischen beiden Einrichtungen.

Dr. Wolfgang Gehrke (l.) und Dr. Olivier Bartheye

ABB.: FI CODE / W. GEHRKE

IM RAHMEN EINES Forschungsaufenthalts besuchte Dr. Wolfgang Gehrke, Laborleiter für Quantencomputing am Forschungsinstitut CODE der Universität der Bundeswehr München, vom 22. April bis 9. Mai 2025 die École de l'air et de l'espace im südfranzösischen Salon-de-Provence. Gastgeber war das Centre de Recherche de l'École de l'Air (CREA), an dem auch das Centre d'Excellence Cyberdéfense Aérospaziale (CEC) angesiedelt ist. Ziel des Aufenthalts war der wissenschaftliche Austausch zu aktuellen Entwicklungen im Bereich Quantencomputing sowie die Vertiefung der deutsch-französischen Forschungskooperation.

Während seines Aufenthalts nahm Dr. Gehrke am „Tag der Forschung" des CREA teil. Unter dem Leitthema „Harmonizing sensors, AI, and humans to shape intelligent systems of tomorrow" diskutierten Forschende aus Wissenschaft und Industrie neue Ansätze zur Verbindung von Sensorik, künstlicher Intelligenz und menschlichen Faktoren in sicherheitskritischen Anwendungen. Dabei ergaben sich zahlreiche Anknüpfungspunkte für zukünftige Kooperationen.

Ein weiterer Schwerpunkt lag auf der akademischen Lehre. Dr. Gehrke hielt einen Fachvortrag mit dem Titel „ZX-calculus as an approach to quantum computing" vor Wissenschaftlerinnen und Wissenschaftlern des CREA. Darin stellte er moderne Konzepte des Quantencomputings sowie grafische Methoden wie das ZX-Kalkül vor. Aufbauend darauf führte er eine zweistündige Gastvorlesung für Kadetten der Offizierschule durch, die auf großes Interesse stieß.

Darüber hinaus präsentierte Dr. Gehrke praktische Beispiele realer Quantenüberlegenheit und diskutierte mit französischen Kolleginnen und Kollegen die Entwicklung eines Curriculums zum Quantencomputing für Studierende der École de l'air et de l'espace. Am Ende des Besuchs bekräftigen sowohl CREA als auch CODE den Wunsch nach weiterem Austausch sowie gemeinsamen Aktivitäten in Forschung und Lehre auch über den Bereich Quantencomputing hinaus. ■

ABB.: ADOBE STOCK / HAMDEE

Nachwuchs-förderung

Chancen und Angebote

Studienpreis des Forschungsinstituts CODE 2025

Design and Optimization of a Multi-Agent System for Traceable Large Language Model-Driven Decision-Making in Cyber-Physical Systems: TADS

Preisträger Leutnant zur See Justin Svrakic (m.) mit Vizepräsident Prof. Dr. Geralt Siebert, Dr. Michael Tagscherer (Giesecke+Devrient GmbH), Prof. Dr. Stefan Pickl (Forschungsgruppe COMTESSA) und dem Leitenden Direktor des FI CODE, Prof. Dr. Wolfgang Hommel (v. l. n. r.).

Das Forschungsinstitut Cyber Defence und Smart Data (FI CODE) zeichnet gemeinsam mit der Firma Giesecke+Devrient GmbH die Masterarbeit von Herrn Justin Svrakic mit dem CODE-Studienpreis 2025 aus. In seiner Arbeit *„Design and Optimization of a Multi-Agent System for Traceable Large Language Model-Driven Decision-Making in Cyber-Physical Systems: TADS“* befasst sich der Absolvent des Masterstudiengangs Informatik mit einer wichtigen Fragestellung aktueller KI-basierter Systeme, nämlich der nachvollziehbaren und regelkonformen Entscheidungsfindung großer Sprachmodelle in missionskritischen cyber-physischen Systemen.

GROSSE SPRACHMODELLE zeigen in vielen Anwendungsfeldern ein hohes Potenzial für kontextbasierte Entscheidungsunterstützung. Gleichzeitig erschweren ihre probabilistische Funktionsweise, fehlende Transparenz und mögliche Inkonsistenzen eine sichere Nutzung in missionskritischen Umgebungen. Gerade dort ist es jedoch essenziell, dass Entscheidungen nicht nur korrekt, sondern auch überprüfbar, erklärbar und eindeutig an Regeln und Erfahrungswissen gebunden sind.

Die Masterarbeit entstand in Zusammenarbeit mit Fraunhofer Singapore Research Ltd und war mit einem mehrmonatigen Auslandsaufenthalt vor Ort verbunden. In diesem internationalen Forschungskontext wurde die Arbeit an realitätsnahen Fragestellungen im Umfeld autonomer Systeme und missionskritischer Anwendungen ausgerichtet. Der enge Austausch mit dem dortigen Forschungsteam ermöglichte es, architektonische Fragestellungen nicht nur theoretisch, sondern auch mit Blick auf praktische Einsatzszenarien zu untersuchen.

Kern der Arbeit ist die Konzeption des *Traceable Agentic Decision-Making System* (TADS). TADS beschreibt eine Multi-Agenten-Architektur, die Case-Based Reasoning und Retrieval-Augmented Generation systematisch kombiniert und diese durch strukturierte Reasoning- und Verifikationsmechanismen erweitert, um Entscheidungen großer Sprachmodelle nachvollziehbar zu machen. Neben einer fall- und dokumentenbasierten Wissensgrundlage setzt TADS gezielt das Prinzip von Chain-of-Thought ein, um Entscheidungsprozesse in explizite, schrittweise Argumentationspfade zu überführen. Ergänzend wird eine Chain-of-Verification genutzt, um diese Argumentationspfade systematisch zu prüfen, zu hinterfragen und mit formalen Richtlinien sowie Missionsvorgaben abzugleichen. Entscheidungen werden damit nicht nur auf frühere Fälle und dokumentierte Regeln, sondern auch auf transparent strukturierte und verifizierte Begründungsschritte zurückgeführt.

Ein zentrales Architekturprinzip ist die strikte Trennung von Entscheidungserzeugung, Validierung und Ausführung. Während ein Agent zunächst einen Lösungsvorschlag auf Basis ähnlicher Fälle generiert, überprüft ein separater Evaluierungsagent diesen Vorschlag gegen dokumentierte Regeln und Einsatzvorgaben. Bei Regelverstößen wird der Vorschlag iterativ überarbeitet, bis eine konforme Entscheidung erreicht ist. Unvalidierte Vorschläge können somit zu keinem Zeitpunkt direkt ausgeführt werden.

Neben dem konzeptionellen Entwurf wurde TADS prototypisch in einer simulierten Umgebung umgesetzt. In einem Aufklärungs- und Überwachungsszenario wurde untersucht, wie stark frühere Entscheidungsfälle das Systemverhalten beeinflussen und in welchem Maß die integrierte Validierungsschleife die Einhaltung von Richtlinien sicherstellt.

Die experimentelle Evaluation zeigt, dass historische Fälle einen messbaren Einfluss auf die Entscheidungsfindung haben, gleichzeitig aber durch die architektonisch verankerte Validierung keine Regelverletzungen zugelassen werden. Damit demonstriert die Arbeit, dass adaptive Entscheidungsfindung und formale Nachvollziehbarkeit durch geeignete Systemarchitektur miteinander vereinbar sind.

Mit seiner Masterarbeit leistet Justin Svrakic einen wichtigen Forschungsbeitrag zu vertrauenswürdiger Künstlicher Intelligenz im Bereich Cyber Defence. Die Arbeit verbindet theoretische Grundlagen, einen klar strukturierten Architekturansatz sowie eine fundierte prototypische Umsetzung und adressiert damit ein hochaktuelles und anspruchsvolles Forschungsproblem.

Der CODE-Studienpreis wurde im Rahmen der großen Masterfeier am 13. Dezember 2025 auf dem Campus der Universität der Bundeswehr München durch den Vizepräsidenten Prof. Geralt Siebert im Beisein des Leitenden Direktors des FI CODE, Prof. Wolfgang Hommel, des Gründers der COMTESSA Forschungsgruppe, Prof. Stefan Pickl, sowie von Dr. Michael Tagscherer (Giesecke+Devrient GmbH) verliehen. ■

ABB.: UNIVERSITÄT DER BUNDESWEHR MÜNCHEN / SIEBOLD

Studienpreise der Universität der Bundeswehr München

Die Universität der Bundeswehr München vergibt jedes Jahr mehrere Studienpreise, die von unterschiedlichen Partnern gestiftet werden. Mit dem Studienpreis des Forschungsinstituts CODE werden seit 2018 herausragende Master-Absolventinnen und -Absolventen mit einer einschlägigen Arbeit aus dem Themenspektrum Cyber Defence ausgezeichnet. Er wird gestiftet von der Giesecke+Devrient GmbH und ist mit 1.000 € dotiert. ■

Die Preisträger der letzten Jahre

Jahr	Preisträger	Schwerpunkt der Arbeit
2018	Christian Siegert	Automatisiertes Aufspüren von IT-Sicherheitslücken
2019	Philipp Sammeck	Sicherheitsanalyse eines elektronischen Tresorschlosses
2020	Robert Jurisch-Eckardt	Entwicklung eines Systems zur Bekämpfung von Cybercrime
2021	Martin Lukner	Synthetisierung von Malware-Spuren für die digitale Forensik
2022	Lars Fuchs	Effiziente Nutzbarmachung von Schwachstellen in Telekommunikationsendgeräten
2023	Hannes Ludwig	An Approach to Creating Adversarial Samples
2024	Annika S.	Szenarioanalyse im Rahmen des Projekts NEWSROOM
2025	Justin Svrakic	Design and Optimization of a Multi-Agent System for Traceable Large Language Model-Driven Decision-Making in Cyber-Physical Systems: TADS

Studieren am Forschungsinstitut CODE

Der **Masterstudiengang Cyber-Sicherheit** am FI CODE der Universität der Bundeswehr München befasst sich mit Informationsverarbeitungs-Prozessen, deren Planung, formaler Modellierung, Implementierung und Einsatz mit einem Fokus auf technische und organisatorische Informationssicherheit. Neben fundierten theoretischen Methoden werden insbesondere auch praxisrelevante Fähigkeiten – etwa zur Identifizierung und Beseitigung von sicherheitsrelevanten Schwachstellen, zur Entwicklung und Implementierung von Sicherheitskonzepten und zur Erkennung und Abwehr von Angriffen auf IT-Systeme – vermittelt. Zudem werden rechtliche und ethische Fragestellungen sowie ausgewählte Themen rund um den Faktor Mensch in der Informationssicherheit behandelt.

Die Bundeswehr fördert zivile Studierende mit einem **Stipendium für den Masterstudiengang Cyber-Sicherheit** an der UniBw M. Voraussetzungen für die Förderung sind ein Studium (Bachelor oder Diplom (FH)) im MINT-Bereich sowie die erfolgreiche Teilnahme an einem Auswahlverfahren des Assessment-Centers für Führungskräfte der Bundeswehr. Neben Studiengängen auf Exzellenzniveau und einer hervorragenden Betreuungsquote durch Lehrpersonal bietet die UniBw M ihren Studierenden eine Vielzahl von Freizeitaktivitäten und Annehmlichkeiten. Günstige Wohnmöglichkeiten in einer der lebenswertesten und vielseitigsten Städte Deutschlands runden die Vorzüge ab.

Weitere Informationen

Master Cyber-Sicherheit:
https://go.unibw.de/mcyb

Stipendium der Bundeswehr:
https://go.unibw.de/stipendium-mcyb

Promotionen 2025

Rudy Milani

„Advanced Automation for Comprehensible Causal Explanations of Reinforcement Learning Agents“

IN DEN LETZTEN JAHREN wurde der Einsatz von Reinforcement Learning durch die Verfügbarkeit leistungsfähiger Rechenressourcen und fortschrittlicher Methoden vorangetrieben, was zu Durchbrüchen in Bereichen wie dem autonomen Fahren, der Medizin und der Finanzwirtschaft geführt hat. Diese Fortschritte gehen jedoch oft auf Kosten der Transparenz, was zu einem Vertrauensverlust bei den menschlichen Nutzern führt. Die Arbeit von Rudy Milani befasst sich mit diesem Problem und schlägt Auto-BENEDICT vor, eine neuartige Methodik, die darauf ausgelegt ist, automatisch kausale Erklärungen für die Handlungen von Agenten im modellfreien Reinforcement Learning zu generieren. Die bereitgestellten Erklärungen beantworten sowohl „Warum“- als auch „Warum nicht“-Fragen und erhöhen so die Verständlichkeit der Entscheidungen der Agenten.

Rudy Milani wurde im Juli 2025 bei Juniorprof. Dr. Maximilian Moll promoviert. Derzeit ist er in der Forschungsgruppe COMTESSA als wissenschaftlicher Mitarbeiter beschäftigt. ■

ABB.: ADOBE STOCK / AH. GIEL; PRIVAT

Michael Mundt

„Cyber-Bedrohungsanalyse weist den richtigen Weg zu einer effizienten und effektiven Milderung der Gefahr des Datendiebstahls“

IM FOKUS STEHT EIN aktuelles Muster von Cyberkriminellen. Sie exfiltrieren sensible Daten, erpressen das Opfer, verkaufen die Daten weiter oder beides. Die Vorstellung eines Konzepts zum Schutz vor Diebstahl und die Untersuchung von Methoden zur Bewusstmachung aktueller Cyberbedrohungen sind Bestandteile der Dissertation. Zudem umfasst sie die Integration in ein bestehendes ISMS und die Analyse der Struktur eines Simulationszyklus. Die Lösung besteht darin, die Simulation laufen zu lassen, bevor ein Angreifer diesen spezifischen Angriffsvektor verwendet. Hierfür werden die Wechselwirkungen zwischen OT und IT betrachtet und es wurde überprüft, dass diese Lösung innerhalb der geltenden Grenzen europäischer Regulierung eingesetzt werden kann. Zudem wurde der Nachweis der Umsetzbarkeit erbracht.

Michael Mundt wurde im April 2025 bei Prof. Dr. Harald Baier promoviert. Er arbeitet bei dem privatwirtschaftlichen Unternehmen Esri Deutschland GmbH und ist derzeit als Gastakademiker im Team der Professur Digitale Forensik tätig. ■

Philipp J. Rösch

„Enhancing Conceptual Understanding in Vision-Language Models“

VISION-LANGUAGE (VL)-Modelle verbinden Bild und Text, scheitern jedoch regelmäßig an Konzepten wie räumlichen Beziehungen, Farbzuweisungen und Größen von Objekten. Diese Dissertation begegnet dem Defizit durch einen konzeptspezifischen Ansatz. Es wird ein *Positional Pre-Training* und ein *Hard Negative Contrastive Learning*-Framework eingeführt, wodurch Modelle gezwungen werden, komplexere Zusammenhänge zu erlernen. Ergänzend wird einen neuer Benchmark-Datensatz präsentiert. Die Ergebnisse belegen eine deutliche Steigerung der Genauigkeit und bieten erstmals eine Methode, um diverse Konzepte präzise in VL-Anwendungen zu integrieren.

Philipp J. Rösch wurde im Juni 2025 bei Prof. Dr. Michaela Geierhos promoviert und ist am Institut für Verteilte Intelligente Systeme als wissenschaftlicher Leiter für Künstliche Intelligenz beschäftigt. ■

ABB.: PRIVAT (2); PHILIPP J. RÖSCH; FOTO PÖTTER;

Sergej Schultenkämper

„Informationspreisgabe im Web: Entwicklung eines Gefährdungsmodells für den digitalen Zwilling“

PREISGEGEBENE INFORMATIONEN im Web – ganz gleich wie unscheinbar – können in Kombination mit anderen Datenpunkten ein erhebliches Gefährdungspotenzial und damit deutliche Sicherheitsrisiken mit sich bringen. Die Dissertation adressiert das Problem mit einem Framework, das Informationen aus unterschiedlichen Profilen mittels datengetriebener Aggregationsverfahren zu konsistenten digitalen Zwillingen zusammenführt. Auf dieser Grundlage wird ein Gefährdungsmodell entwickelt, das aufzeigt, wie attraktiv eine Person als potenzielles Angriffsziel für Identitätsdiebstahl ist und wie einfach ein Spear-Phishing-Angriff auf sie zugeschnitten werden kann.

Sergej Schultenkämper wurde im Oktober 2025 bei Prof. Dr. Michaela Geierhos promoviert und arbeitet im Career@BI-Programm als Lehrkraft für besondere Aufgaben an der HSBI sowie als Data Scientist bei der wonk.ai GmbH. ■

Laura Stojko

„Personalizing User Interfaces of Large Interactive Displays for Intercultural Groups in Semi-Public Areas“

GROSSE INTERAKTIVE DISPLAYS in halböffentlichen Räumen können von vielen verschiedenen Personen genutzt werden, wobei jede einzelne Person einen eigenen kulturellen Hintergrund mitbringt, der die User Experience solcher Displays beeinflusst. Diese Dissertation entwickelte einen Personalisierungsansatz, der die interkulturellen Gestaltungspräferenzen kleiner Nutzergruppen berücksichtigt, durch Gruppenmodellierung (Aggregation) Datenschutzanforderungen wahrt und es dem Display ermöglicht, sich selbstständig an Gruppen anzupassen. Eine Mixed-Methods-Evaluation validierte den Ansatz und zeigte eine deutliche Verbesserung der User Experience.

Laura Stojko wurde im August 2025 bei Prof. Dr. Michael Koch promoviert. Derzeit ist sie am Institut für Softwaretechnologie als Postdoktorandin bei Prof. Dr. Wolfgang Hommel beschäftigt. ■

ABB.: ADOBE STOCK / NAJMA'S VISUAL

Addendum

Publikationen, Aktivitäten und Organisation

Prof. Dr. Harald Baier

Digitale Forensik

PUBLIKATIONEN

GÖBEL, T., BAIER, H.: From IaC to IoC – Using Infrastructure as Code (IaC) to Generate Synthetic Datasets of Compromised (IoC) Linux Systems for Use in Digital Forensics. Digital Threats: Research and Practice 6 (4), S. 1-21, 2025.

GÖBEL, T., BREITINGER, F., BAIER, H.: Optimising data set creation in the cybersecurity landscape with a special focus on digital forensics: Principles, characteristics, and use cases. Forensic Science International: Digital Investigation 52, 301882 2025.

KLIER, S., BAIER, H.: Media source similarity hashing (MSSH): A practical method for large-scale media investigations. DFRWS APAC, Forensic Science International: Digital Investigation 54, 301977, 2025.

KLIER, S., BAIER, H.: Metrics Matter – Source Camera Forensics for Large-Scale Investigations. Digital Threats: Research and Practice 6 (4), S. 1-21, 2025.

KLIER, S., BAIER, H.: Source Camera Identification – Do we have a gold standard? Forensic Science International: Digital Investigation 52, 301858, 2025.

LOHRE, K., BAIER, H., HARDI, L., ATTENBERGER, A.: Towards reliable data in the scope of unmanned aircraft systems. Forensic Science International: Digital Investigation 53, 301914, 2025.

RZEPKA, L., BAIER, H.: Quality of Inconsistencies in (Windows) Memory Dumps. In: Proceedings of the 15th SPRING graduate workshop of the special interest group Security – Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI), Nuremberg (Germany), April 2025.

RZEPKA, L., OTTMANN, J., STOYKOVA, R., FREILING, F., BAIER, H.: A scenario-based quality assessment of memory acquisition tools and its investigative implications. DFRWS EU, Forensic Science International: Digital Investigation 52, 301868, 2025.

WOLF, D., BAIER, H.: Bringing AI into ForTrace++ – A Framework for Automatic Data Synthesis. 15th SPRING graduate workshop, 2025.

LEHRE

1162	**Erweiterte Digitale Forensik (WT)***
3824	**Digitale Forensik (HT)**
5001/1009	**Seminar Digitale Forensik (WT + FT)**
5501/1009	**Seminar Forensische Methoden der Informatik (HT)**
5505	**IT-Forensik (FT)**

MESSEN, TAGUNGEN, SEMINARE

- Vorbereitung und Moderation des CAST-Workshops Forensik/Internetkriminalität am 20.11.2025, Darmstadt, URL: https://cast-forum.de/workshops/infos/355
- Vortrag From IaC to IoC – Using Infrastructure as Code (IaC) to Generate Synthetic Datasets of Compromised (IoC) Linux Systems for Use in Digital Forensics. 13th IT Security Incident Management & IT Forensics (IMF) 2025, 16.09.25, Albstadt

WEITERE FUNKTIONEN

- Vorsitzender des Prüfungsausschusses des Masterstudiengangs Cyber-Sicherheit an der UniBw M
- Co-Vorsitzender des Technical Programme Committee des Digital Forensics Research Workshop (DFRWS) USA 2025
- Mitglied im Fakultätsrat Informatik
- Mitglied im Fachgremium IT-Forensik der IHK für München und Oberbayern (bundesweit zuständig für die Prüfung im Rahmen der Öffentlichen Bestellung und Vereidigung von Sachverständigen auf dem Teilgebiet IT-Forensik), gegründet und eingerichtet im Mai 2025
- Mitglied im Programmbeirat des Masterstudiengangs ‚Digitale Forensik' der Hochschule Albstadt-Sigmaringen
- Mitglied im Steering Committee der Konferenz IT Security Incident Management & IT Forensics (IMF), https://www.imf-conference.org
- Mitglied im Organisation Committee der IMF 2025
- Gutachter für das Journal Digital Investigation
- Gutachter für das Journal Computers & Security

Mitglied des Programmkomitees

- Digital Forensics Research Workshop (DFRWS) EU 2025
- Digital Forensics Research Workshop (DFRWS) APAC 2025
- IT Security Incident Management & IT Forensics (IMF) 2025
- IFIP Working Group 11.9 International Conference on Digital Forensics 2025
- CAST-GI Promotionspreis 2025
- GI-Skill

** Trimesterangaben:*

HT: Herbsttrimester (Okt. – Dez.)
WT: Wintertrimester (Jan. – Mär.)
FT: Frühjahrstrimester (Apr. – Jun.)

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

PUBLIKATIONEN

SARAFOV, V., MARKVICA, D., BRUNTHALER, S.: TEPHRA: Principled Discovery of Fuzzer Limitations, in ASE '25: 40th IEEE/ACM International Conference on Automated Software Engineering, ASE 2025, November 16-20, 2025, Seoul, South Korea ASE 2025, L. Böhme Marchel Zhang, Ed., 2025.

FORSCHUNGSPROJEKTE

APERITIF – Analysis Pipeline for Effective Vulnerability Identification Through Fuzzing

Im Rahmen des Projekts APERITIF erforscht µCSRL gemeinsam mit der Forschungsgruppe PATCH von Prof. Dr. Kinder neue, hochskalierende und automatische Schwachstellenanalyse-Verfahren durch Fuzzing auf Datacenter-Ebene. Unterstützt durch einen eigenen Cluster analysiert das Team neue Möglichkeiten zur Parallelisierung und Optimierung von einzelnen Fuzzern.

Gefördert durch: BMVg/BAAINBw
Laufzeit: 2021–2025

DEMISEC – Detecting Malicious Implants in Source Code)

Moderne Software enthält eine Reihe von externen Open-Source-Komponenten, die von vielen verschiedenen Personen entwickelt wurden. Beinhaltet auch nur eine dieser Komponenten potenziell bösartigen Code, ist die Sicherheit des gesamten Produkts gefährdet. Im Projekt DEMISEC wird untersucht, wie sich böswillige Änderungen an Quellcode erkennen lassen, bevor sie den Entwicklungsprozess unterwandern können

Gefördert durch: BMVg/BAAINBw
Laufzeit: 2021–2025

DEPS (Dependable Production Environments with Software Security)

Das Projekt DEPS erforscht neuartige Techniken, um Software effizient an Hardware zu binden. Die dadurch geschützten Systeme sind zum einen deutlich resilienter gegenüber regulären Angriffen und erschweren zum anderen gängige Reverse-Engineering-Techniken, um geistigen Diebstahl entweder ganz zu verhindern oder durch Kostenexplosionen unökonomisch werden zu lassen.

Gefördert durch: Österreichische Forschungsförderungsgesellschaft (FFG), Software Competence Center Hagenberg
Laufzeit: 2022–2025

LEHRE

1009 **Seminar Language-based Security (WT)**

1009 **Seminar Optimization of Programming Languages (HT)**

1010 **Maschinennahe Programmierung (WT)**

3647 **Compilerbau (HT + WT)**

55071 **Language-based Security (FT)**

MESSEN, TAGUNGEN, SEMINARE

- 23. Kolloquium aus Programmiersprachen in Feldkirchen-Westerham
- 41. Workshop der GI Fachgruppe Programmiersprachen in Bad Honnef
- 40. IEEE/ACM International Conference in Automated Software Engineering (ASE)
- 61. Workshop der IFIP Working Group 2.4 „Software Implementation Technology"
- 11. Workshop Amsterdam Security Workshop der VU Amsterdam (AMSec)
- NATO Conference on Cyber Conflict, CyCon 2025 (Invited talk)

PREISE UND AUSZEICHNUNGEN

- ACM SIGSOFT Distinguished Paper Award

WEITERE FUNKTIONEN

- Panel Member NATO Conference on Cyber Conflict (CyCon 2025)

Prof. Dr. Michaela Geierhos

Data Science

PUBLIKATIONEN

BABL, F., HENNEN, M., MURAUER, J., GEIERHOS, M.: Splitting Negatively Impacts NER Evaluation: Quantifying and Eliminating the Overestimation of NER Performance. In: Che, W., Nabende, J., Shutova, E., Pilehvar, M. T. (Hrsg.). Findings of the Association for Computational Linguistics: ACL 2025. Association for Computational Linguistics. 2025. S. 9724-9738.

BELLGRAU, B., HOMMEL, W., GEIERHOS, M., KNÜPFER, M.: Gemeinsam mit KI gegen neue Cyberbedrohungen: Ein Bericht zur CODE-Jahrestagung 2024. Zeitschrift für Außen- und Sicherheitspolitik. 2025.

FISCHER, M. T., SCHLEGEL, U., KEIM, D. A., ALTMANN, S., GROTE, C., REUTER, P., COLEMAN, G., GEIERHOS, M., MAORO, F., KLUIN, M., WEINBRUCH, M., ADEN, H. KLEEMANN, S., TAHRAOUI, M., LOUBAN, A.,ARNDT, M., SCHÖNROCK, S., BRANDNER, L. T., HIRSBRUNNER, S. D., LOH, W., YILMAZ, Y.: Anforderungen an vertrauenswürdige KI-Methoden in polizeilichen Anwendungen. Berlin. DIN Media GmbH. 2025. 68 S.

GEIERHOS, M., MAORO, F.: Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen (VIKING): Teilvorhaben: Erklärbarkeit vertrauenswürdiger KI-Sprachmodelle für den transparenten Gebrauch bei Sicherheitsbehörden zur Textklassifikation. 2025. 27 S.

GEIERHOS, M.: Künstliche Intelligenz: Potenziale, Risiken und Regulierung. Vergaberecht – Zeitschrift für das gesamte Vergaberecht (VergabeR). 2025. Nr. VS-Sonderheft 5a/2025. S. 684-698.

HÖLLIG, J., GEIERHOS, M.: Utility Meets Privacy: A Critical Evaluation of Tabular Data Synthesizers. IEEE Access. 2025.

LEE, Y. S., BOTHE, H., GEIERHOS, M.: A Guide to Feature-preserving Pseudonymization of Profile Pictures. In: Yurish, Sergey Y. (Ed.). Big Data Analytics & Applications. Barcelona, Spanien. IFSA Publishing, S. L.. International Frequency Sensor Association (IFSA). 2025. S. 14-17.

MAORO, F., GEIERHOS, M.: Contestable AI for Criminal Intelligence Analysis: Improving Decision-Making Through Semantic Modeling and Human Oversight. Frontiers in Artificial Intelligence. Vol. 8. 2025.

MURAUER, J., KRISHNAKUMAR, R., TORNOW, S., GEIERHOS, M.: Feedback Connections in Quantum Reservoir Computing with Mid-Circuit Measurements. 2025 IEEE International Conference on Quantum Computing and Engineering (QCE). Piscataway, NJ. IEEE. 2025.

NIELSEN, A., WALTER, A., SIENKNECHT, M., VEHMEYER, B., GEIERHOS, M.: Measuring the Multidimensionality of Absorptive Capacity through AI-enabled Website Analysis. 32nd Innovation and Product Development Management Conference 2025 Proceedings. 2025.

NIELSEN, A., WALTER, A., VEHMEYER, B.: Measuring the Multidimensionality of Absorptive Capacity through AI-Enabled Website Analysis. Annual Meeting of the Academy of Management (85., 2025, Kopenhagen). 2025.

SEEMANN, N., LEE, Y. S., BOTHE, H., GEIERHOS, M.: FI-CODE@GermEval Shared Task 2025: LLM Prompting for Augmentation of Underrepresented Classes. In: Wartena, C., Heid, U. (Hrsg.). Proceedings of the 21st Conference on Natural Language Processing (KONVENS 2025). Hannover. HsH Applied Academics. 2025. S. 327–336.

SOARES DE SOUZA, A., MEISSNER, A., GEIERHOS, M.: Towards JPEG-Compression Invariance for Adversarial Optimization. Proceedings of the 20th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications – Volume 3: VISAPP. Setúbal, Portugal. SciTePress. 2025. S. 166-177.

STEININGER, C., GÖTZ, L., SCHOPP, M.: How Accessible Is Cybersecurity Training?: A Survey on the Accessibility, Capabilities, and Technology Stack of Cyber Ranges. IEEE Access. Vol. 13. 2025. S. 203980-204039.

VEHMEYER, B., GEIERHOS, M.: Connection Is all You Need! Mining and Linking Disparate Data Sources for Collaboration Network Analysis. Proceedings of the 27th International Conference on Enterprise Information Systems – Volume 1: ICEIS. Setúbal, Portugal. SciTePress. 2025. S. 210-217.

FORSCHUNGSPROJEKTE

VIKING – Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen

Das Teilprojekt „Erklärbarkeit vertrauenswürdiger KI-Sprachmodelle für den transparenten Gebrauch bei Sicherheitsbehörden zur Textklassifikation“ widmet sich im Rahmen des Verbundprojekts VIKING der Erforschung vertrauenswürdiger KI-Methoden zur Textklassifikation.

Gefördert durch: Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR)
Laufzeit: 01/2022 – 03/2025

TACR – Technische Adaption von Cyber Ranges für die militärische Nutzung

In der F&T-Studie wird untersucht, wie der Bedarf von Dienststellen in der Bundeswehr an Trainingsanlagen für das digitale Umfeld, sogenannten Cyber Ranges, gedeckt werden kann. Dazu werden verschiedene Use Cases und Cyber-Range-Produkte geprüft und evaluiert. Zusätzlich werden ebenso Szenare im militärischen Kontext entwickelt und in einer Übung praktisch geprobt.

Gefördert durch: BMVg/WTD81
Laufzeit: 10/2023 – 09/2025

KiTIE – Kooperationskompetenz im Technologietransfer – Identifikation und Evaluation von Partnern anhand von Patentinformationen

Das Projekt entwickelt ein Tool zur Identifikation von Kooperationspartnern für außeruniversitäre Forschungseinrichtungen. Das Ziel ist es, eine effektive und effiziente Partnerfindung im Technologietransfer zu ermöglichen sowie eine transparente und eigenverantwortliche Beteiligung aller Akteure zu fördern.

Gefördert durch: Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR)
Laufzeit: 02/2023 – 07/2026

NAWI – News-Artikel und Wissen

Das Projekt NAWI beschäftigt sich mit der Wissensgewinnung und -modellierung aus News-Artikeln.

Laufzeit: 12/2021 – 11/2026

KI-basierter Sprachsignal-Decoder

Das Ziel dieser Machbarkeitsstudie ist die prototypische Umsetzung eines neuronalen Netzes zur Dekodierung bestehender Vocoder-Daten zur Verbesserung der Empfangsqualität.

Laufzeit: 09/2021 – 12/2026

AutoTrainer milCR – Automatisierte Trainingserstellung militärischer Cyber Ranges

Mit der F&T-Studie wird untersucht, wie spezifisch auf die Bedürfnisse der Bundeswehr angepasste Cyber-Range-Trainings entwickelt werden können. Die Studie baut auf den Ergebnissen des CD&E-Projekts „Cyber Range Bw“ auf und untersucht die Möglichkeiten zur automatisierten Generierung von Environments und Szenarien für militärisch genutzte

Cyber Ranges. Dabei kommen die neuesten Technologien aus den Bereichen Infrastructure as Code, Konfigurationsmanagement und Automatisierung zum Einsatz. In diesem Kontext werden auch Trainingsszenarios erstellt und in praktisch durchgeführten Übungen mit militärischem Personal erprobt.

Gefördert durch: BMVg/WTD81
Laufzeit: 10/2025 – 06/2028

FINEST – KI-gestützte Sprachverarbeitungsumgebung

Maschinelle Übersetzungen haben durch den Einsatz von Large Language Models (LLMs) signifikante Fortschritte erfahren. Diese Modelle sind jedoch meist auf allgemeine Sprachdaten trainiert und zeigen Defizite bei der Übersetzung hochspezialisierter Fachterminologie. Dies betrifft insbesondere sicherheitskritische und technische Kontexte, in denen Übersetzungsfehler gravierende Folgen haben können. Ziel des Projekts ist es, LLMs durch domänenspezifisches Fine-Tuning für den Einsatz in Fachübersetzungen zu optimieren und systematisch zu evaluieren. Ein ergänzender Schwerpunkt liegt auf der Untersuchung des Einflusses von Anonymisierung auf die Übersetzungsqualität.

Gefördert durch: BMVg/WIWeB
Laufzeit: 12/2025 – 12/2028

LEHRE

1144: **Knowledge Discovery in Big Data (FT + HT)**

3850: **Natural Language Processing (WT + FT)**

3851: **Information Retrieval (WT)**

3852: **Anwendungsgebiete der Data Science (FT + HT)**

3853: **Analyse unstrukturierter Daten (HT)**

MESSEN, TAGUNGEN, SEMINARE

- Bodensee Business Forum 2025 (Graf-Zeppelin-Haus, Friedrichshafen)
- Tagung „Cybersicherheit, Resilienz und Souveränität" (Akademie für Politische Bildung Tutzing in Zusammenarbeit mit der Gesellschaft für Informatik e.V. und der Initiative D21 e.V.)
- DeepLearn 2025 (Universität Maia, Portugal)
- KI@BW 2025 (HSU, Hamburg)

WEITERE FUNKTIONEN

- Mitglied in der Studiengangskommission Master Cyber-Sicherheit
- Projektleitung der „Deutschen Biographie" der Historischen Kommission bei der BAdW
- Mitglied im Allgemeinen Rat der Katholischen Akademie in Bayern
- Gutachterin für die Europäische Kommission
- Gutachterin für VDI/VDE Innovation + Technik
- Gutachterin für die Österreichische Forschungsförderungsgesellschaft (FFG)

Mitglied im Programmkomitee

- ACL 2025 – Annual Meeting of the Association for Computational Linguistics
- LREC 2026 – International Conference on Language Resources and Evaluation
- PATTERNS 2025 – International Conference on Pervasive Patterns and Applications

Prof. Dr. Marta Gomez-Barrero

BioML: Biometrics and Machine Learning Lab

PUBLIKATIONEN

DEMIR, O., SCHUTH, T., GOMEZ-BARRERO, M.: Hash-based iris protection using maximum entropy binary codes and CNNs, Proc. International Conference of the Biometrics Special Interest Group (BIOSIG), 2025.

LEIBLER, A., GOMEZ-BARRERO, M., MAYER, H.: Closing the Gap Between Real and Anonymized Data For Training Face Detection Models, Proc. Int. Workshop on Biometrics and Forensics (IWBF), 2025.

LEHRE

26681 **Selected Topics in Deep Learning (FT)**

42111 **Biometric Recognition (HT)**

42112 **Selected topics in Biometric Recognition (HT)**

42121 **Deep Learning (FT)**

42122 **Selected Topics in Deep Learning for IT-Security (FT)**

MESSEN, TAGUNGEN, SEMINARE

- IEEE Int. Conference of the Biometrics Special Interest Group (BIOSIG) – General Chair + Vortrag von Osman Demir
- IEEE Int. Workshop on Biometrics and Forensics (IWBF) – General Chair
- IEEE Int. Joint Conference on Biometrics (IJCB) – Publications Chair
- EAB Online Seminar on Fingerprint Presentation Attack Detection – Chair
- EAB-CITeR Martigny Biometrics Workshop – Co-Chair

WEITERE FUNKTIONEN

- General Chair der International Conference of the Biometrics Special Interest Group (BIOSIG, https://biosig.de/)
- Vorsitzende der BIOSIG Special Interest Group der Gesellschaft für Informatik (GI)
- Stellvertretende Vorsitzende der European Association for Biometrics (EAB)
- Mitglied des IARP TC4 Conference Committee, des IEEE Biometrics Council Security and Privacy Technical Committee, und des IEEE Information and Forensics Technical Committee
- Delegierte des Deutschen Instituts für Normung (DIN) in ISO/IEC SC37 JTC1 SC37 für Biometrie
- Co-Affiliation Norwegian University of Science and Technology (NTNU)

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

PUBLIKATIONEN

BELLGRAU, B., HOMMEL, W., GEIERHOS, M., KNÜPFER, M.: Gemeinsam mit KI gegen neue Cyberbedrohungen: Ein Bericht zur CODE-Jahrestagung 2024. Zeitschrift für Außen- und Sicherheitspolitik. 2025.

BÜTTNER, A., GRUSCHKA, N., BROEN, S. S., PÖHN, D.: Authentication Inconsistencies Across Online Services: A Multi-Scenario Security Analysis. In: Coppens, Bart; Volckaert, Bruno; Naessens, Vincent; Sutter, Bjorn de (Ed.). Availability, Reliability and Security. Cham. Springer. 2025. S. 166-180.

FIETKAU, J., STOJKO, L.: Privacy Customization in a Social Sharing Tool: Where Academic Publications Meet Social Platforms. Mensch und Computer 2025. Gesellschaft für Informatik e.V.. 2025.

HOFMEIER, M., HAUNSCHILD, I., HOFMEIER, M., HOMMEL, W.: Individual Technology Commitment and the Rating of Usability and Trustworthiness of Electronic Signature Systems. HCI for Cybersecurity, Privacy and Trust. Cham. Springer. 2025. S. 42–55. Lecture Notes in Computer Science; 15815.

NEUMAYR, T., YIGITBAS, E., AUGSTEIN, M., HERDER, E., STOJKO, L., STRECKER, J., SEITZ, J.: ABIS 2025 – International Workshop on Personalization and Recommendation. Mensch und Computer 2025. Gesellschaft für Informatik e.V.. 2025.

PÖHN, D.: Then I clicked something – Helping Users to Report Security Incidents with Digital Identity Wallets. Open Identity Summit (2025, Neubiberg). 2025. S. 55-69. Lecture Notes in Informatics.

PÖHN, D., GRUSCHKA, N.: Qualitative In-Depth Analysis of GDPR Data Subject Access Requests and Responses from Major Online Services. Proceedings of the 11th International Conference on Information Systems Security and Privacy, Volume 1: ICISSP. Setúbal, Portugal. Science and Technology Publications. 2025. S. 149-156.

PÖHN, D., LÜKEN, H.: Got Ya!: Sensors for Identity Management Specific Security Situational Awareness. Proceedings of the 11th International Conference on Information Systems Security and Privacy. Setúbal, Portugal. Science and Technology Publications. 2025. S. 141-148., 1.

PÖHN, D., STREIBER, R.: Legal and ethical considerations when conducting phishing experiments in Germany. International Cybersecurity Law Review. 2025.

SHARIF, A., ANSAROUDI, Z. E., SCIARRETTA, G., PÖHN, D., MOLLAEEFAR, M., HOMMEL, W., RANISE, S.: Protecting Digital Identity Wallet: A Threat Model in the Age of eIDAS 2.0. In: Collart-Dutilleul, Simon; Ouchani, Samir; Cuppens, Nora; Cuppens, Frédéric (Ed.). Risks and Security of Internet and Systems. Cham. Springer. 2025. S. 89-106. Lecture Notes in Computer Science; 15456.

STEININGER, Ch.: Creating a Framework for Platform-Independent Cyber Range Scenarios. NOMS 2025-2025 IEEE Network Operations and Management Symposium (2025, Honolulu). 2025. S. 4.

STEININGER, Ch., GÖTZ, L., SCHOPP, M.: How accessible is cybersecurity training? A survey on the accessibility, capabilities, and technology stack of Cyber Ranges. IEEE Access. 2025.

STEINKE, M., HOMMEL, W.: A Protocol for Ultra-Low-Latency and Secure State Exchange Based on Non-Deterministic Ethernet by the Example of MVDC Grids. Electronics. 2025.

STOJKO, L.: Group Modeling Cultural Dimension Values for Intercultural Personalization. UMAP Adjunct '25: Adjunct Proceedings of the 33rd ACM Conference on User Modeling, Adaptation and Personalization. New York. Association for Computing Machinery. 2025. S. 317-321.

STOJKO, L.: Personalizing User Interfaces of Large Interactive Displays for Intercultural Groups in Semi-Public Areas. 2025. xxii, 200 S.

ZIEGLER, L., GRABATIN, M., PÖHN, D., HOMMEL, W.: Designing a security incident response process for self-sovereign identities. EURASIP Journal on Information Security. Vol. 2025. 2025. Ss. 12.

FORSCHUNGSPROJEKTE

6G-life

Mit dem Abschluss der ersten Phase des Projekts 6G-life wurde ein ganzheitlicher Forschungsansatz erfolgreich realisiert, in dessen Rahmen innovative Konzepte in skalierbarer Kommunikation, neuartigen Methoden, flexiblen Softwarearchitekturen und adaptiver Hardware entwickelte wurden. Die Forschungsarbeiten förderten den Grundgedanken der Mensch-Maschine-Kollaboration, während in allen Bereichen die Anforderungen an Latenz, Resilienz, Sicherheit und Nachhaltigkeit als Querschnittsthemen parallel berücksichtigt wurden.

Drittmittelgeber: BMFTR (Unterauftrag der TU München)
Laufzeit: 12/2022 – 08/2025

Anwendungsorientierte Technologiepotentiale für Cyber/IT

Das Ziel der F&T-Maßnahme „Anwendungsorientierte Technologiepotentiale für Cyber/IT“ ist es, Forschungsideen und Innovationen zu identifizieren, divergierende Interessen, Ziele und Methoden im Bereich der Forschung von Cybersicherheit und Cyberverteidigung zusammenzuführen sowie die Sektoren-übergreifende Kooperation im Bereich Technologiemonitoring im Cyber-Cluster voranzutreiben.

Drittmittelgeber: Wehrtechnische Dienststelle für Informationstechnologie und Elektronik in der Bundeswehr (WTD81)
Laufzeit: 07/2024 – 12/2026

ACSE LTE – Airborne Cybersecurity Enhancement Long Term Evolution

Airborne Cybersecurity Enhancement (ACSE) LTE (Long Term Evolution) war das Folgeprojekt des Ende 2023 abgeschlossenen ACSE-Projekts. Wie sein Vorgänger war ACSE LTE Teil der Forschungskooperation zwischen dem FI CODE und Airbus Defence and Space. Der Fokus dieses Projekts lag auf der Anwendung der im Vorgänger gewonnen Erkenntnisse zu sicherer Flugzeugkommunikation für taktische Datenlinks.

Drittmittelgeber: Airbus Defence and Space
Laufzeit: 01/2024 – 12/2025

AutoTrainer milCR – Automatisierte Trainingserstellung militärischer Cyber Ranges

Mit der F&T-Studie Automatisierte Trainingserstellung militärischer Cyber Ranges wird untersucht, wie spezifisch auf die Bedürfnisse der Bundeswehr angepasste Cyber Range Trainings entwickelt werden können. Die Studie baut auf den Ergebnissen des CD&E-Projekts „Cyber Range Bw“ auf und untersucht die Möglichkeiten zur automatisierten Generierung von Environments und Szenarien für militärisch genutzte Cyber Ranges. Dabei kommen die neuesten Technologien aus den Bereichen Infrastructure as Code, Konfigurationsmanagement und Automatisierung zum Einsatz. In diesem Kontext werden auch Trainingsszenarios erstellt und in praktisch durchgeführten Übungen mit militärischem Personal erprobt.

Drittmittelgeber: WTD81
Laufzeit: 10/2025 – 06/2028

DEFINE – DC-Netze für eine sichere Energieversorgung

Moderne Stromnetze sind stark abhängig von einer zuverlässigen Informations- und Kommunikationstechnologie und ohne diese nicht betreibbar. Jede IT-Komponente birgt aber eine Angriffsfläche im Cyber-Raum, die möglichst gering gehalten werden muss. Am FI-CODE wird im Projekt DEFINE aktuell an der automatischen Erkennung von Angriffen auf die Kommunikationsinfrastruktur von Stromnetzen geforscht, um diese sicher betreiben zu können.

Drittmittelgeber: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Projektlaufzeit: 01/2021 – 12/2026

Entwicklung und Integration realer Cyber-Sicherheitsvorfälle in Cyber-Range-Trainings

Um auf die zunehmende Bedrohung durch Cyberangriffe reagieren zu können, ist die effektive Schulung von Incident-Response- und Forensik-Fachkräften von zentraler Bedeutung. Cyber-Ranges bieten eine sichere Umgebung, um Cyber-Sicherheitsvorfälle zu simulieren. Dadurch können technische Fähigkeiten, Werkzeuge sowie Prozesse und Rollen abseits von realen Systemen und Incidents erprobt werden. Ziel dieses Projekts ist es, ein Konzept zu entwickeln, das die systematische Überführung von realen Cyber-Sicherheitsvorfällen in diese Trainingsumgebung ermöglicht.

Gefördert durch: Landesamt für Sicherheit in der Informationstechnik (LSI)
Laufzeit: 05/2025 – 06/2028

LIONS – Ledger Innovation and Operation Network for Sovereignty

Das Projekt LIONS baut eine Forschungsplattform zur Erhöhung von Resilienz und Digitaler Souveränität in der Digitalisierung mittels Distributed-Ledger-Technologien auf. Als Teil des interdisziplinären Forschungsprojekts steht für die Forschungsgruppe dabei das Thema Self-Sovereign Identity Management und die technische Unterstützung der Projektpartner im Mittelpunkt.

Drittmittelgeber: dtec.bw
Laufzeit: 01/2021 – 12/2026

MuQuaNet – Das Quanten-Netzwerk im Großraum München

Im Projekt MuQuaNet entsteht im Großraum München ein Test- und Demonstrationsnetz für Quantenkommunikation. Ziel ist es, Technologien zur sicheren Schlüsselverteilung mittels Quantum Key Distribution (QKD) zu erforschen und nahtlos in bestehende Infrastrukturen zu integrieren. Dabei werden kommerzielle Systeme erprobt, miniaturisierte Komponenten entwickelt und Management- sowie Sicherheitsmechanismen für künftige skalierbare Quantennetze umgesetzt.

Drittmittelgeber: dtec.bw
Laufzeit: 10/2020 – 12/2026

ROLORAN – Resilient Operation of LoRa Networks

Dieses Projekt evaluiert die Nutzbarkeit der weitreichenden, energieeffizienten und robusten Funktechnologie LoRaWAN. Neben Softwareanalysen zur Protokollhärtung und Messreihen zu Sendereichweite, Stör- und Ortbarkeit werden prototypische Einzelgeräte und Gesamtsysteme entwickelt. Augenmerk liegt hierbei auf Kooperationen zu den Szenarien Sturzflutfrühwarnung und Krisenkommunikation.

Drittmittelgeber: dtec.bw
Laufzeit: 01/2021 – 12/2026

TACR – Technische Adaption von Cyber-Ranges für die militärische Nutzung

In der F&T Studie Technische Adaption von Cyber-Ranges für die militärische Nutzung wurde untersucht, wie der Bedarf von Dienststellen in der Bundeswehr an Trainingsanlagen für das digitale Umfeld, sogenannten Cyber Ranges, gedeckt werden kann. Dazu wurden verschiedene Use-Cases und Cyber-Range-Produkte geprüft und evaluiert. Zusätzlich wurden ebenso Szenare im militärischen Kontext entwickelt und in einer Übung praktisch geprobt.

Gefördert durch: WTD81
Laufzeit: 10/2023 – 06/2025

LEHRE

1006 **Einführung in die Informatik 1 (HT)**

1007 **Einführung in die Informatik 2 (WT)**

1640 **Identitätsmanagement (WT+FT, PD Pöhn)**

1785 **Sicherheit in der Informationstechnik (WT, PD Pöhn)**

3459 **Ausgewählte Kapitel der IT-Sicherheit (WT+FT)**

3479 **Methoden der Cyber Security (HT, PD Pöhn)**

5501 **Seminar Anwendungs- und Softwaresicherheit (FT)**

5501 **Seminar Informationssicherheitsmanagement (HT)**

5507 **Sichere vernetzte Anwendungen (FT)**

5508 **Sicherheitsmanagement (FT)**

MESSEN, TAGUNGEN, SEMINARE

- Workshop Chair EDId @ ARES 2025 (PD Pöhn)
- Workshop Chair OID 2025 (PD Pöhn)
- DKE BKT-Sitzung Frankfurt (PD Pöhn)
- ABIS Workshop auf der Mensch und Computer 2025 (Dr. Stojko)

WEITERE FUNKTIONEN

- Dekan der Fakultät für Informatik
- Mitglied im Betriebsausschuss des Deutschen Forschungsnetzes

Mitglied des Programmkomitees

- IEEE/IFIP International Symposium on Integrated Network Management
- IEEE/IFIP Network Operations and Management Symposium
- DFN-Konferenz Sicherheit in vernetzten Systemen
- International Workshop on Frontiers in Availability, Reliability and Security
- Annual Privacy Forum (PD Pöhn)
- International Workshop on Emerging Digital Identities (PD Pöhn)
- Open Identity Summit (PD Pöhn)
- Workshop on Network Security Operations (PD Pöhn)
- International Conference on Network and System Security (PD Pöhn)
- International Symposium on Security and Privacy in Social Networks and Big Data (PD Pöhn)
- Workshop on Trends in Digital Identity (PD Pöhn)
- Computer Science Review (PD Pöhn)
- Computers & Security (PD Pöhn)
- Journal of Information Security and Applications (PD Pöhn)
- Technology in Society (PD Pöhn)
- IEEE Access (PD Pöhn)
- EURASIP Journal on Information Security (PD Pöhn)

Prof. Dr.-Ing. Mark Manulis

Privacy and Applied Cryptography Lab

PUBLIKATIONEN

CHEN, L., MENG, L., MANULIS, M., TIAN, Y., ZHANG, Y.: Attribute-Based Key Exchange with Optimal Efficiency. CANS 2025.

LIU, J., MANULIS, M.: Fast SNARK-based Non-Interactive Distributed Verifiable Random Function with Ethereum Compatibility. ASIA CCS 2025.

MAIRE, J., PULVAL-DADY, A.: Blind ECDSA from the ECDSA Assumption. IACR Communications in Cryptology 2025.

MANULIS, M. (Ed.): Applied Cryptography and Network Security Workshops — ACNS 2025 Satellite Workshops. ACNS 2025, Parts I, II, III.

MANULIS, M., NARTZ, H.: Distributed Asynchronous Remote Key Generation. ACNS 2025.

VALBUSA, F., KRENN, S., LORÜNSER, T., RAMACHER, S.: Seamless Post-Quantum Transition: Agile and Efficient Encryption for Data-at-Rest. SECRYPT 2025.

FORSCHUNGSPROJEKTE

SCANDIUM

Im Projekt werden Methoden zur Verbesserung der Zusammenarbeit zwischen deutschen Strafverfolgungsbehörden untersucht, die mit komplexen und ressourcenintensiven Ermittlungsaufgaben konfrontiert sind. Obwohl diese Behörden grundsätzlich zur Zusammenarbeit bereit sind, hindern sie strenge Vorschriften daran, sensible Informationen direkt auszutauschen. Die Koordination muss daher so erfolgen, dass die Vertraulichkeit gewahrt bleibt und gleichzeitig eine effiziente Nutzung der begrenzten Ressourcen ermöglicht wird.

Gefördert durch: Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)
Laufzeit: 08/2025 – 07/2028

LIONS – Ledger Innovation and Operation Network for Sovereignty

Das interdisziplinär ausgerichtete Forschungsprojekt baut eine Plattform für die Erforschung von Distributed-Ledger-Technologie als eine Technologie der Digitalisierung zur Erhöhung von Resilienz und digitaler Souveränität auf. Dazu gehört unter anderem Weiterentwicklung von verteiltem und souveränen Identity Management unter Sicherheits- und Schutzaspekten in Anwendungsbereichen wie IoT, Web-Anwendungen und eGovernance.

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 01/2021 – 12/2026

LEHRE

55481 **Modern Cryptography (WT)**

55482 **Research Trends in Cryptography (WT)**

55631 **Private Data Processing (FT)**

55632 **Private Authentication and Messaging (HT)**

55633 **Privacy Enhancing Cryptography in Practice (FT + HT)**

MESSEN, TAGUNGEN, SEMINARE

- Dagstuhl-Seminar „Guardians of the Galaxy: Protecting Space Systems from Cyber Threats“ (eingeladener Teilnehmer)
- ACNS 2025 (Workshop Chair)
- ACM ASIACCS 2025 (Vortragender)

WEITERE FUNKTIONEN

- Associate Editor für IEEE Transactions on Information Forensics and Security (IEEE TIFS)
- Associate Editor für International Journal of Information Security (IJIS), Springer
- Gastprofessor an der University of Surrey, Großbritannien

Prof. Dr.-Ing. Carmen Mas Machuca

Kommunikationsnetze (COMNET)

PUBLIKATIONEN

AGARWAL, R., BERMUDEZ SERNA, C., SHARMA, A., MAS-MACHUCA, C.: Resilient Cascaded Optical Access Networks: An Urban Case-Study. 2025 25th Anniversary International Conference on Transparent Optical Networks (ICTON). Piscataway, NJ. IEEE. 2025.

BERMUDEZ SERNA, C., JANARDHANAN, S., DOĞAN, E., SHARMA, A., MAS-MACHUCA, C.: Dependency Analysis of Optical Access Networks on Electrical Distribution Networks. 2025 25th Anniversary International Conference on Transparent Optical Networks (ICTON). Piscataway, NJ. IEEE. 2025. S. 1-5.

JANARDHANAN, S., CHEN, Y. MAS-MACHUCA, C.: PyRBD++: An Open-Source Fast Reliability Block Diagram Evaluation Tool. International Workshop on Resilient Networks Design and Modeling (15., 2025, Trondheim). Piscataway, NJ. IEEE. 2025. S. 1-7.

JANARDHANAN, S., ERHARDT, J., MAS-MACHUCA, C.: PyRobust: An Open-Source Robustness Surface Generation Tool. 2025 25th Anniversary International Conference on Transparent Optical Networks (ICTON). Piscataway, NJ. IEEE. 2025.

JANARDHANAN, S., GOMEZ RYFKA, A. I., MAS-MACHUCA, C.: Investigating the Correlation between Minimal Cut Set and Flow availabilities. WueWoWAS. 2025.

JANARDHANAN, S., PATRICIA, J., KELLERER, W., MAS-MACHUCA, C.: Interactive Demonstration of an Open-Source Dependability Suite for Communication Networks. 2025 25th Anniversary International Conference on Transparent Optical Networks (ICTON). Piscataway, NJ. IEEE. 2025.

MAS-MACHUCA, C., WENNING, M.: Towards Resilient and Secure QKD networks. 2025 25th Anniversary International Conference on Transparent Optical Networks (ICTON). Piscataway, NJ. IEEE. 2025.

SAMONAKI, M., ÇIÇEK, M. E., BERMUDEZ SERNA, C., KELLERER, W., MAS MACHUCA, C.: SDR-MDNet: A tool for Survivable Demand Routing in Multi-Domain Networks. EuCNC & 6G Summit (2025, Poznan). 2025.

SAMONAKI, M., YEH, Y.-H., KELLERER, W., MAS-MACHUCA, C.: Cost-effective and reliable multi-period optical network planning comparing capacity and topology upgrades. Journal of Optical Communications and Networking. Vol. 17. 2025. No. 9. S. D30-D42.

SHARMA, A., AGARWAL, R., BERMUDEZ SERNA, C., MAS-MACHUCA, C.: Comparative Analysis of Type-C Approaches in Protected PON. International Workshop on Resilient Networks Design and Modeling (15., 2025, Trondheim). Piscataway, NJ. IEEE. 2025. S. 1-8.

WENNING, M., BERL, J., FEHENBERGER, T., MAS-MACHUCA, C.: Comparison of distributed and centralized quantum key management systems for meshed QKD networks. Journal of Optical Communications and Networking. Vol. 17. 2025. No. 2. S. A224-A233.

WENNING, M., BERL, J., FEHENBERGER, T., MAS-MACHUCA, C.: Improving End-to-end Key Security in Trusted Node-based QKD Networks with Secret Sharing. Optical Fiber Communication Conference (OFC) 2025. Optica Publishing Group. 2025. S. W1J. 6.

FORSCHUNGSPROJEKTE

FRONT-RUNNER – Flexible and Resilient Optical Network Technologies for Resistant & Uninterrupted Access Networks

Das geplante Projekt leistet einen wesentlichen Beitrag zur Erreichung der Förderpolitischen Ziele der Fördermaßnahme „Resilienz – Resiliente Digitale Systeme“, indem es die Resilienz optischer Zugangsnetze gegenüber externen und internen Störungen durch automatisierte Prozesse erhöht.

Gefördert durch: BMFTR
Laufzeit: 01/2023 – 12/2025

PONGO – Passive optische Netze der nächsten Generation

Der Beitrag der Gruppe besteht in der Konzeption und Entwicklung eines neuen Planungsinstruments, das die Kostenbewertung der vorgeschlagenen Lösungen unterstützt und erweitert wird, um den besten Migrationspfad unter Berücksichtigung der aktuellen optischen Zugangsnetze zu ermitteln.

Gefördert durch: BMFTR
Laufzeit: 06/2024 – 05/2027

HyperCORE

Im Projekt sollen Technologien zur Erhöhung der Übertragungskapazität unter Berücksichtigung aller drei verfügbaren physikalischen Dimensionen, Zeit (Kanaldatenraten), Frequenz (Kanalwellenlängen) und Raum (Anzahl räumlicher Kanäle) untersucht und im Hinblick auf Energieeffizienz optimiert werden.

Gefördert durch: BMFTR
Laufzeit: 07/2024 – 06/2027

SUSTAINET-Advance

COMNET hat sich zum Ziel gesetzt, einen Beitrag zur Modellierung, Implementierung und Bewertung resilienter Netzwerke zu leisten. Resilienz berücksichtigt nicht nur Ausfälle des Kommunikationsnetzwerks selbst, sondern auch Ausfälle anderer Infrastrukturen, wie beispielsweise Stromnetze. Die gegenseitigen Abhängigkeiten zwischen den beiden Netzwerken werden berücksichtigt, um neue Architekturen und Lösungen vorzuschlagen.

Gefördert durch: BMFTR
Laufzeit: 07/2024 – 06/2027

LEHRE

4088 **Kommunikationsnetze I**

4138 **Kommunikationsnetze II**

4140 **Photonische Netze**

WEITERE FUNKTIONEN

- Member of the IEEE Germany Section Executive Committee
- External advisory member NORCICS project
- External advisory member ECO-eNET project
- OSA JOCN Associate editor
- IEEE TNSM Guest editor of the special issue "Robust and Resilient Future Communication Networks"
- Host of ITG FG KT 3.3 Workshop “FONDAC: Future optical networks design and control”
- External advisory member IoTalentum project
- OFC’25 TPC Member
- ECOC’25 TPC Member
- ONDM’25 TPC Co-chair

Juniorprof. Dr.
Maximilian Moll

Operations Research – Prescriptive Analytics

PUBLIKATIONEN

ARNOLD, J., MOLL, M., PICKL, S.: Extended SPEC: Analysing Loss Functions for Forecasting Sparse Time Series. International Conference on Operations Research 2024.

EHRLICH, J., MOLL, M., PICKL S.: A generalized trade reduction mechanism. Central European Journal of Operations Research. pp. 1-20. 2025. doi: 10.1007/s10100-025-00969-w

DORSCH, J., GODDU, M. K., NAVE, K., VIERKANT, T., COECKELBERGH, M., GÜRTLER, P., URBAN, P., SPANG, F., MOLL, M.: Against AI welfare: Care practices should prioritize living beings over AI. AI Magazine, 46(3), e70016. 2025. doi: 10.1002/aaai.70016

MILANI, R., NISTOR, M. S., MOLL, M., PICKL, S.: On the Correlation and Predictability of Topological Measures in Transportation Networks. Oper. Res. Forum 6, 82. 2025. doi: 10.1007/s43069-025-00471-8

MOLL, M., DORSCH, J.: A systematic review of human-centered explainability in reinforcement learning: transferring the RCC framework to support epistemic trustworthiness. Human-Intelligent Systems Integration. 2025. doi: 10.1007/s42454-025-00084-w

MOLL, M., KUNCZIK, L.: A case study for cyber-attack detection using quantum variational circuits. Quantum Machine Intelligence 7.1. pp. 1-23. 2025. doi: 10.1007/s42484-025-00277-1

SUN, W., RIPP I., BORRMANN, A., MOLL, M., FAIRHUST, M.: Touch-driven advantages in reaction time but not in performance in a cross-sensory comparison of reinforcement learning. Heliyon, 11(1). 2025. doi: 10.1016/j.heliyon.2024.e41330

WELLER, D., MOLL, M.: Neurocomputing.: Assessing Hyperparameter Importance in Reinforcement Learning. 2025. doi: 10.1016/j.neucom.2025.131770

FORSCHUNGSPROJEKTE

NATO SET-IST-339: Investigations of Military Applications of Quantum Computing

Die NATO-Arbeitsgruppe untersucht das Potenzial von Quantencomputing für militärische Anwendungen, insbesondere zur Verarbeitung und Auswertung von Sensordaten. Im Fokus stehen Quantenalgorithmen für Optimierung, Machine Learning und Datenanalyse, um Lagebilder zu verbessern und Entscheidungsprozesse zu beschleunigen.

Laufzeit: 04/2024 – 04/2027

NATO SAS-181: Exploiting Reinforcement Learning to Achieve Decision Advantage

Die Forschungsgruppe arbeitet daran, wie Reinforcement Learning (RL) und Approximate Dynamic Programming die sicherheits- und verteidigungsrelevante Entscheidungsfindung der NATO verbessern können. Fachleute aus Regierung, Militär und Wissenschaft analysieren bestehende RL-Ansätze, entwickeln ein Rahmenwerk für RL-basierte Entscheidungsunterstützung und leiten bewährte Verfahren ab. Zudem formuliert die Gruppe Empfehlungen für zukünftige Forschung und weitere Aktivitäten der NATO Science and Technology Organization.

Laufzeit: 02/2023 – 05/2026

LEHRE

2031-V2	**Mathematik für Verwaltungsinformatiker**
10362	**Operations Research**
14901	**Ausgewählte Kapitel des Operations Research und der Entscheidungstheorie**
29941	**Ausgewählte Kapitel des Data-driven Optimization**
29942	**Quantum Machine Learning & Optimization**
33961	**Data Mining und IT-basierte Entscheidungsunterstützung**
552611	**Digitalisierung**

MESSEN, TAGUNGEN, SEMINARE

- GOR-Arbeitsgruppe Simulation und Optimierung komplexer Systeme, 06.11.2025 – 07.11. 2025
- The International Conference on Operations Research 2025 (OR2025) Stream: Simulation and Quantum Computing, 02.09.2025 – 05.09.2025

WEITERE FUNKTIONEN

- Fellow der Bayerischen Wissenschaftsallianz für Friedens-, Konflikt- und Sicherheitsforschung
- Koordinator Hochbegabtenförderung an der Universität der Bundeswehr München
- Arbeitsgruppenleiter „Simulation und Optimierung komplexer Systeme“, Deutsche Gesellschaft für OR

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

PUBLIKATIONEN

GHODSI, S., SEYEDI, A., LE QUY, T., KARIMI, F., NTOUTSI, E.: A Deep Latent Factor Graph Clustering with Fairness–Utility Trade-off Perspective. IEEE Big Data, 2025.

KUMAR, V., SINGH, P., NTOUTSI, E.: Mitigating Semantic Drift: Evaluating LLMs' Efficacy in Psychotherapy through In-context Conversational Dialogue Summarization Leveraging MITI Code. International Joint Conference on Neural Networks (IJCNN), 2025.

NTOUTSI, E.: The Multifaced Nature of Bias in AI – Impact on Model Generalization, Robustness, and Fairness. In: SCHÄFFER, B.; LIEDER, F. R. (eds.), Maschinen wie wir? Springer Gabler, Wiesbaden, 2025.

PANAGIOTOU, E., QIAN, H., MARX, S., NTOUTSI, E.: Generative AI-augmented offshore jacket design: Integrated approach for mixed tabular data generation under scarcity and imbalance. Automation in Construction, 2025.

PANAGIOTOU, E., RONVAL, B., ROY, A., BOTHMANN, L., BISCHL, B., NIJSSEN, S., NTOUTSI, E.: TABFAIRGDT – A Fast Fair Tabular Data Generator using Autoregressive Decision Trees. IEEE International Conference on Data Mining (ICDM), 2025.

ROY, A., RIZOU, S., PAPADOPOULOS, S., NTOUTSI, E.: Achieving Socio-Economic Parity through the Lens of the EU AI Act. ACM Conference on Fairness, Accountability, and Transparency (FAccT), 2025.

SWATI, S., ROY, A., PANAGIOTOU, E., NTOUTSI, E.: MMM-fair: An Interactive Toolkit for Exploring and Operationalizing Multi-Fairness Trade-offs. ACM Conference on Information and Knowledge Management (CIKM), 2025.

XU, Z., KANDANAARACHCHI, S., ONG, C. S., NTOUTSI, E.: Fairness Evaluation with Item Response Theory. The Web Conference (WWW), 2025.

FORSCHUNGSPROJEKTE

STELAR – Spatio-Temporal Linked Data Tools for the Agri-Food Data Space

Entwicklung eines Knowledge Lake Management Systems (KLMS) zur Unterstützung von fairen und KI-fähigen Daten durch Datenqualitätsbewertung, Bias-Erkennung und Erklärbarkeit, validiert anhand realer Anwendungsfälle im Agrar- und Ernährungsbereich

Gefördert durch: Europäische Union (Horizon Europe, HORIZON-CL4-2021-DATA-01-03)
Laufzeit: 09/2022 – 08/2025

MAMMoth – Multi-Attribute, Multimodal Bias Mitigation in AI Systems

Forschung zu Fairness-bewussten KI-Methoden zur Adressierung von Mehrfachdiskriminierung über mehrere geschützte Merkmale hinweg in tabellarischen, Netzwerk- und multimodalen Daten, mit Pilotanwendungen in den Bereichen Finanzwesen, Identitätsverifikation und akademische Netzwerke.

Gefördert durch: Europäische Union (Horizon Europe, HORIZON-CL4-2021-HUMAN-01)
Laufzeit: 11/2022 – 10/2025

LEHRE

2319 **Artificial Intelligence (WT)**

2320 **Responsible Artificial Intelligence (HT)**

2321 **Machine Learning (FT)**

MESSEN, TAGUNGEN, SEMINARE

- Organisatorin, BIAS Workshop, co-located mit der European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD 2025).
- Eingeladene Sprecherin, Brussels Responsible AI Network (BRAIN) Forum: Tackling Multi-dimensional Discrimination in AI.
- Dozentin, AIDA PhD Summer School: Advanced Course on Bias in AI Systems, Thessaloniki, Greece.
- Keynote-Speakerin, CISUC, Coimbra, Portugal: Bias and Fairness in AI – Current and Future Trends.
- Eingeladene Sprecherin, AI Fairness Cluster Meeting, Brüssel: The Multifaceted Nature of Bias in AI – Implications for Generalization, Fairness, and Robustness.
- Panelistin, Munich Security Conference 2025 Side Event „Automating Human Security – Rethinking the Role of AI in Conflict for the Protection of Civilians", München.
- Eingeladene Sprecherin, TRANSFERleben Breakfast Club 2025, München: Towards Trustworthy AI: Technically Robust and Socially Responsible.

WEITERE FUNKTIONEN

- Mitglied in der Studiengangskommission Master Cyber-Sicherheit, UniBw M.
- Vorstandsmitglied und Fakultätsvertreterin, Fakultätentag Informatik (FTI).
- Mitglied, L3S Research Center, Leibniz Universität Hannover.
- Mitglied des Beirats, Weizenbaum-Institut, Berlin.
- Gutachterin, Europäische Kommission.
- Gutachterin, Luxembourg National Research Fund.
- Mitglied der Berufungs- und Auswahlkommissionen, UniBw M sowie nationale und internationale Institutionen.
- Mitglied der Promotionskommissionen, UniBw M sowie nationale und internationale Institutionen.
- Mentorin, MENTality-Programm, UniBw M.
- Mitglied des Programmausschusses internationaler Konferenzen im Bereich Künstliche Intelligenz und Machine Learning (u. a. IJCAI, AAAI, ECML PKDD, PAKDD und FAccT).
- Mitgliedschaften: IEEE, ACM, AAAI, GI.

Prof. Dr. Stefan Pickl

Operations Research – Forschungsgruppe COMTESSA

LEHRE

10245 **Praktikum Operations Research – Entscheidungsunterstützung (WT + FT + HT)**

10252 **Seminar Ausgewählte Kapitel des Operations Research I (WT + FT + HT)**

10371 **Einführung in die Wirtschaftsinformatik (HT)**

10372 **Grundlagen der Informations- und Kommunikationstechnik (HT)**

10401 **Einführung in Business Intelligence (FT)**

12311 **Data Mining und IT-basierte Entscheidungsunterstützung (WT)**

12325 **Praktikum Operations Research – Entscheidungsunterstützung II (WT + FT + HT)**

12326 **Seminar Ausgewählte Kapitel des Operations Research II (FT)**

2038-V1 **KI und datenbasierte Optimierung (FT)**

3481-V1 **Datenwissenschaft und -analyse (FT)**

WEITERE FUNKTIONEN

- Vize-Präsident Deutsches Komitee für Katastrophenvorsorge DKKV
- Beiratsvorsitzender der Deutschen OR Gesellschaft
- Mitglied DEU NATO SAS Panel
- Mitglied Munich Aerospace
- Kuratoriumsmitglied der Hessischen Schülerakademie
- Präsidiumsmitglied VOICE – Bundesverband der IT-Anwender e.V.
- Mitglied der Deutschen Akademie für Technikwissenschaften ACATECH
- Mitglied im Club of Rome

Prof. Dr. Daniel Slamanig

Quantum Safe & Advanced Cryptography Lab

PUBLIKATIONEN

ABE, M., NANRI, M., OHKUBO, M., PEREZ KEMPNER, O., SLAMANIG, D., TIBOUCHI, M.: A Certified-Input Mixnet from Two-Party Mercurial Signatures on Randomizable Ciphertexts. 30th European Symposium on Research in Computer Security – ESORICS 2025.

BORIN, G., CORTE-REAL SANTOS, M., ERIKSEN, J. K., INVERNIZZI, R., MULA, M., SCHAEFFLER, S., VERCAUTEREN, F.: Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies. 31st International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2025.

DEN HOLLANDER, T., KLEINE, S., MULA, M., SLAMANIG, D., SPINDLER, S. A.: More Efficient Isogeny Proofs of Knowledge via Canonical Modular Polynomials. 45th Annual International Cryptology Conference - CRYPTO 2025.

DEN HOLLANDER, T., SLAMANIG, D.: A Crack in the Firmament: Restoring Soundness of the Orion Proof System and More. 31st International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2025.

HANZLIK, L., LAI, Y.-F., MULA, M., PARACUCCHI, E., SLAMANIG, D., TANG, G.: Tanuki: New Frameworks for (Concurrently Secure) Blind Signatures from Post-Quantum Group Actions. 31st International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2025.

SLAMANIG, D.: Privacy-Preserving Authentication: Theory vs. Practice. Privacy and Identity Management. Generating Futures. Privacy and Identity 2024. IFIP Advances in Information and Communication Technology, vol 705. Springer. 2025.

LEHRE

10251 **Seminar Kryptologie (FT + HT)**

39311 **Introduction to Post-Quantum Cryptography (HT)**

39312 **Selected Topics in Post-Quantum Cryptography (WT)**

39313 **Post-Quantum Cryptography in Practice (WT)**

51181 **Foundations of Distributed Systems and Blockchains (WT)**

51182 **Research Topics in Security for Decentralized Systems (WT)**

MESSEN, TAGUNGEN, SEMINARE

- 45th Annual International Cryptology Conference – CRYPTO 2025, Santa Barbara, USA
- 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT 2025, Madrid, Spanien
- 31st International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2025, Melbourne, Australien
- ArcticCrypt 2025, Longyearbyen, Svalbard, Norwegen
- CrypTO-Konferenz, Turin, Italien
- 23rd International Conference on Applied Cryptography and Network Security – ACNS 2025, München
- BIRS Workshop "Isogeny Graphs in Cryptography", Banff, Kanada
- Leuven Isogeny Days 6, Leuven, Niederlande
- 39. Krypto-Tag, Kirchheim b. München
- Young Researcher Crypto Seminar Spring 2025, Konstanz
- Young Researcher Crypto Seminar Fall 2025, Karlsruhe
- SQIparty2025-Workshop, Lleida, Spanien

WEITERE FUNKTIONEN

- Gutachter für die Deutsche Forschungsgemeinschaft (DFG)
- Academic Editor für IET Information Security
- Editor Journal of Universal Computer Science
- Editorial Board Member IACR Communications in Cryptology
- Editorial Board Member Proceedings on Privacy Enhancing Technologies (PoPETs)
- Editorial Board Member Journal of Universal Computer Science
- Co-Organisator des International Workshop on Foundations and Applications of Privacy-Enhancing Cryptography – PrivCrypt 2025, München
- Keynote Speaker an der Australian Summer School on Privacy 2025, Sydney, Australien
- Keynote Speaker am "Workshop on Cryptographic Tools for Blockchains" co-located mit der EUROCRYPT 2025, Madrid, Spanien
- Teilnahme am Panel "Post Quantum Cryptography", Webinar Trust in Digital Life (TDL)
- Teilnahme am Panel "Bringing Privacy Research to Reality", Australian Summer School on Privacy 2025, Sydney, Australien

Mitglied des Programmkomitees

- 31st International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2025)
- 28th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2025)
- 9th International Conference on Cryptology and Information Security in Latin America (LATINCRYPT 2025)
- 32nd Annual ACM Conference on Computer and Communications Security (ACM CCS 2025)
- 31st Australasian Conference on Information Security and Privacy (ACISP 2025)
- 40th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2025)
- 12th ACM Asia Public-Key Cryptography Workshop (APKC 2025)
- 25th Central European Conference on Cryptology (CECC 2025)
- 19th International Conference on Provable and Practical Security (ProvSec 2025)

Prof. Dr. Arno Wacker

Datenschutz und Compliance

PUBLIKATIONEN

BEHRENDT, D., BUSSE, B.: How we use LaTeX in the CrypTool project. TUGboat, vol. 46, no.2, S. 206-212, Annual Conference of the TeX Users Group, July 27, 2025. doi:10.47397/tb/46-2/tb143behrendt-cryptool

DEN HOLLANDER, T., KLEINE, S., MULA, M., SLAMANIG, D., SPINDLER, S. A.: More Efficient Isogeny Proofs of Knowledge via Canonical Modular Polynomials. In: Tauman Kalai, Y., Kamara, S.F. (Eds.), Advances in Cryptology – CRYPTO 2025. Lecture Notes in Computer Science 16000, S. 131-166. Springer, Cham, 2025. doi: 10.1007/978-3-032-01855-7_5

EMPL, P., KOCH, D., DIETZ, M., PERNUL, G.: Digital Twins in Security Operations: State of the Art and Future Perspectives. ACM Computing Surveys. doi: 10.1145/3746279

HÖLZL, R., KLEINE, S., STEPHAN, F.: Improved lower bounds for strong n-conjectures, J. Aust. Math. Soc. 119:1, S. 61-81, 2025. doi: 10.1017/S1446788725000084

KLEINE, S., MATAR, A., SUJATHA, R.: On the $\mathfrak{M}_H(G)$-property. Math. Proc. Cambridge Philos. Soc.179:2, S. 449-501, 2025. doi: 10.1017/S0305004125000325

KLEINE, S., MÜLLER, K.: Fine Selmer groups of modular forms, Abh. Math. Sem. Univ. Hamburg 95/2, S. 93–121, 2025. doi: 10.1007/s12188-025-00292-w

LEHRE

3480 **Sichere Netze und Protokolle (FT)**

55011 **Seminar Vulnerabilities and Attack Vectors (FT +HT)**

55041 **Datenschutz (WT)**

55042 **Privacy Enhancing Technologies (WT)**

55061 **Einführung in die Kryptographie (WT)**

55062 **Kryptoanalyse (WT)**

55091 **Penetration Testing (HT)**

55093 **Praktikum Penetration Testing (WT + FT)**

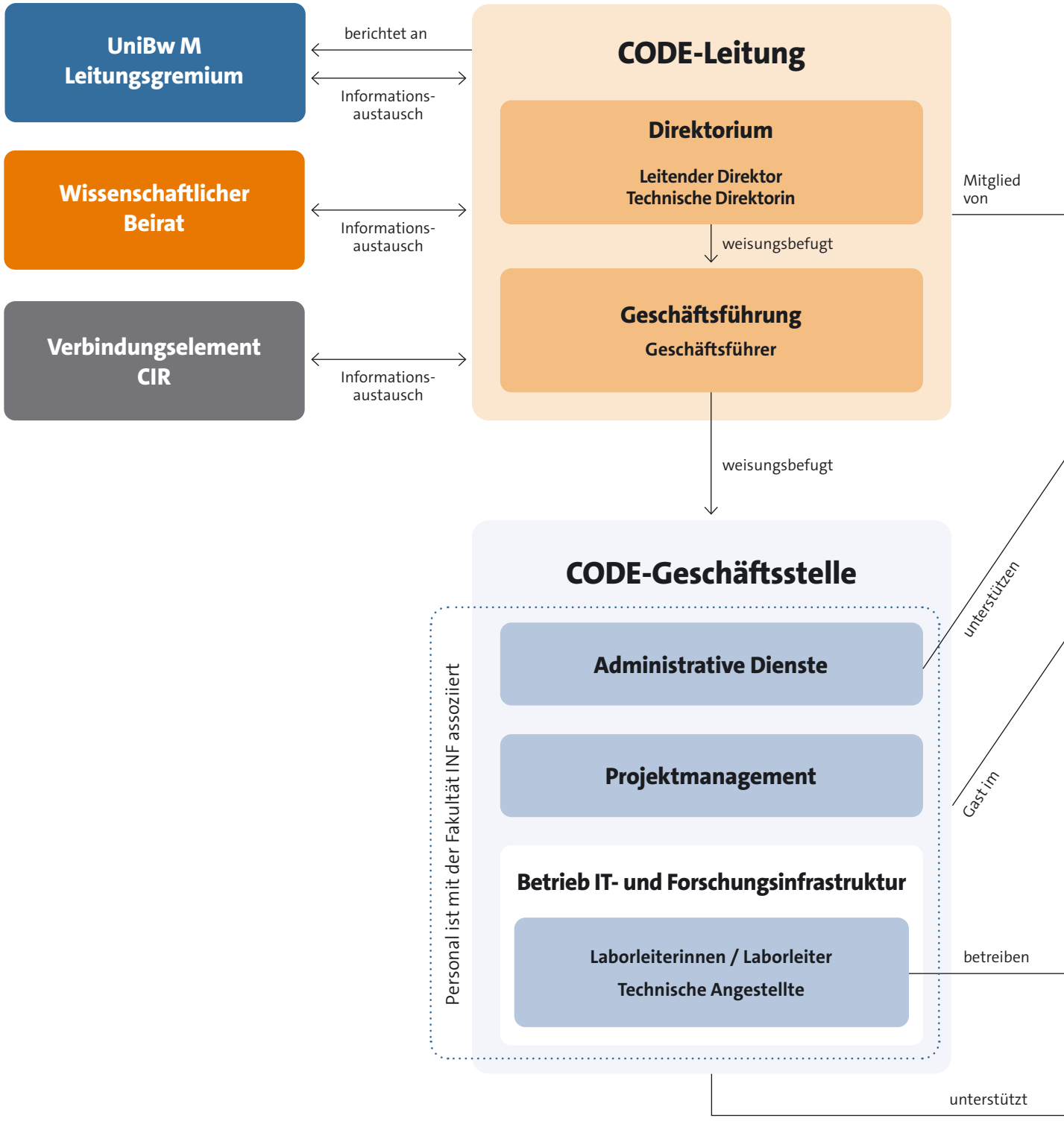
MESSEN, TAGUNGEN, SEMINARE

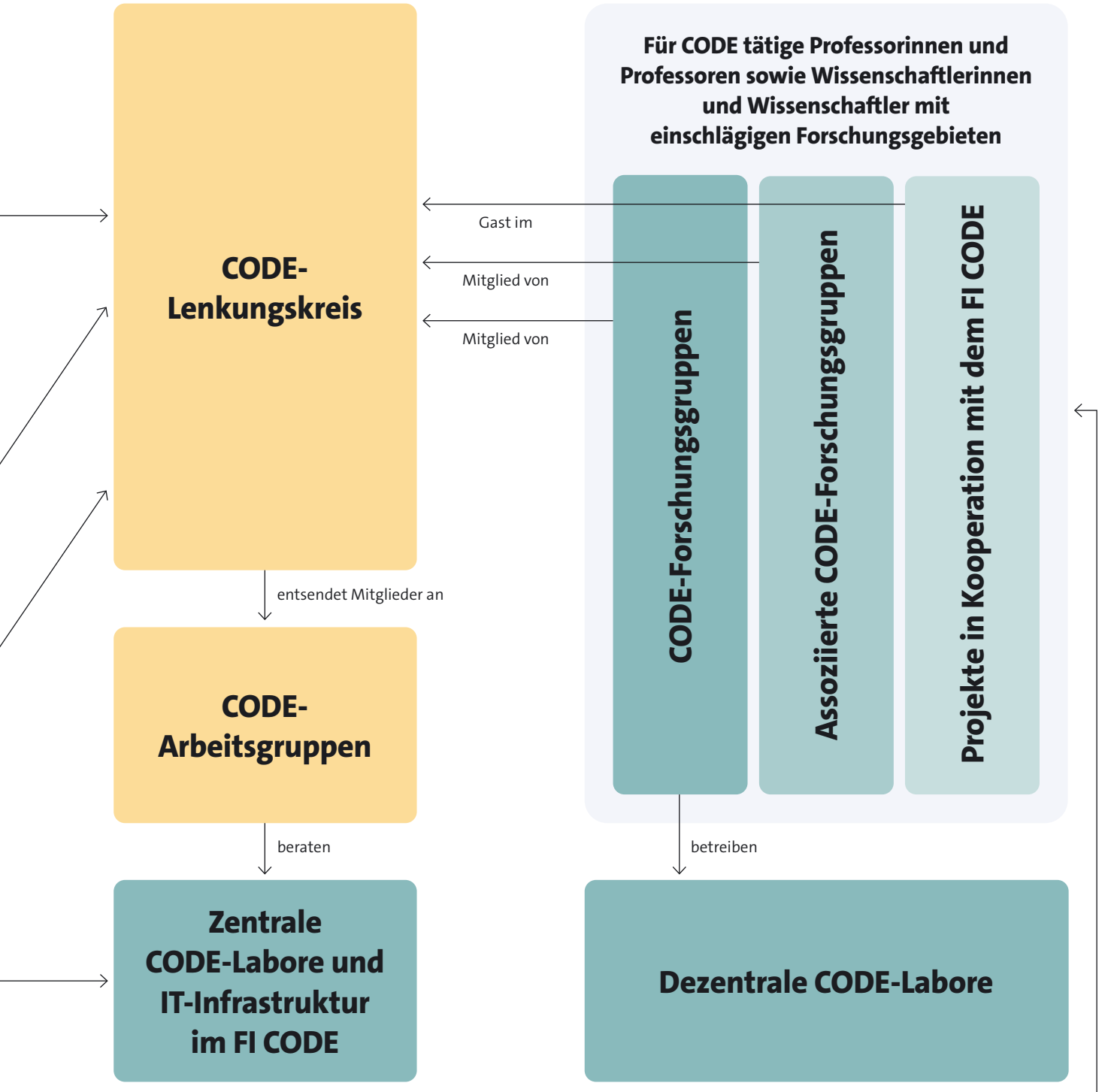
- 01.12.25 – Online-Treffen mit dem Gymnasium Ulricianum Aurich: Professor Wacker stellte seine Forschungsarbeit und des FI CODE vor und diskutierte aktuelle Themen der IT-Sicherheit.

WEITERE FUNKTIONEN

- Leiter des Rechenzentrums der UniBw M

Organisation des FI CODE




CODE-Lenkungskreis
Für CODE tätige Professorinnen und Professoren sowie Wissenschaftlerinnen und Wissenschaftler mit einschlägigen Forschungsgebieten
Gast im
Mitglied von
Mitglied von
CODE-Forschungsgruppen
Assoziierte CODE-Forschungsgruppen
Projekte in Kooperation mit dem FI CODE
entsendet Mitglieder an
CODE-Arbeitsgruppen
beraten
betreiben
Zentrale CODE-Labore und IT-Infrastruktur im FI CODE
Dezentrale CODE-Labore

So erreichen Sie uns

Forschungsinstitut Cyber Defence und Smart Data (CODE)
Universität der Bundeswehr München
Carl-Wery-Straße 18
81739 München

code@unibw.de
+49 89 6004 7300
www.unibw.de/code

LinkedIn: Forschungsinstitut Cyber Defence (CODE)
YouTube: Forschungsinstitut Cyber Defence

Lageplan

Impressum

HERAUSGEBER

Forschungsinstitut CODE
Universität der Bundeswehr München
Carl-Wery-Str. 18
81739 München

LEITUNG DES FI CODE

Prof. Dr. Wolfgang Hommel, Leitender Direktor

Prof. Dr. Michaela Geierhos, Technische Direktorin

Marcus Knüpfer, M. Sc., Geschäftsführer (bis 12/2025)

Stefanie Molnar, M. A., Kommissarische Geschäftsführerin (seit 01/2026)

PD Dr. Daniela Pöhn, Kommissarische Geschäftsführerin (seit 01/2026)

PROFESSUREN AM FI CODE

Prof. Dr. Harald Baier, Professor für Digitale Forensik

Prof. Dr. Stefan Brunthaler, Professor für sichere Software-Entwicklung

Prof. Klaus Buchenrieder, PhD, Professor für Eingebettete Systeme/Rechner in Technischen Systemen

Prof. Dr. Gabi Dreo Rodosek, Professorin für Kommunikationssysteme und Netzsicherheit

Prof. Dr. Michaela Geierhos, Professorin für Data Science

Prof. Dr. Marta Gomez-Barrero, Studiendekanin der Fakultät für Informatik an der UniBw M, Professorin für Maschinelles Lernen

Prof. Dr. Udo Helmbrecht, Honorarprofessor am FI CODE

Prof. Dr. Wolfgang Hommel, Dekan der Fakultät für Informatik an der UniBw M, Professor für IT-Sicherheit von Software und Daten

Prof. Dr. Michael Hutter, Professor für Embedded Systems Security

Prof. Dr.-Ing. Mark Manulis, Prodekan der Fakultät für Informatik an der UniBw M, Professor für Privacy

Prof. Dr. Eirini Ntoutsi, Professorin für Open Source Intelligence

Prof. Dr. Corinna Schmitt, außerplanmäßige Professorin für Secure Communication Systems

Prof. Dr. Daniel Slamanig, Professor für Kryptologie

Prof. Dr. Arno Wacker, Professor für Angewandte Sicherheitsanalysen (vormals Datenschutz und Compliance)

Alle an der Fakultät für Informatik der Universität der Bundeswehr München

CODE-ASSOZIIERTE PROFESSUREN

Prof. Dr. Ulrike Lechner, Professorin für Wirtschaftsinformatik, Fakultät für Informatik

Prof. Dr.-Ing. Carmen Mas Machuca, Professorin für Kommunikationsnetze, Fakultät für Elektrische Energiesysteme und Informationstechnik

Juniorprof. Dr. Maximilian Moll, Juniorprofessor für Operations Research – Prescriptive Analytics, Fakultät für Informatik

Prof. Dr.-Ing. Vladislav Nenchev, Professor für Embedded Systems, Fakultät für Elektrotechnik und Technische Informatik

Prof. Dr. Christoph Peters, Professor für Digital Process Management, Fakultät für Wirtschafts- und Organisationswissenschaften

Prof. Dr. Stefan Pickl, Professor für Operations Research, Fakultät für Informatik

Prof. Dr. Gunnar Teege, Professor für Verteilte Systeme, Fakultät für Informatik

Alle an der Universität der Bundeswehr München

MITGLIEDER DES BEIRATS (IM JAHR 2025)

Aus der Fakultät für Informatik der Universität der Bundeswehr München

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Ulrike Lechner

Prof. Dr.-Ing. Helmut Mayer

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

Weitere Mitglieder

Wolfgang Sachs, IC II 5, Bundesministerium der Verteidigung

Dr.-Ing. Christian Keimel, Airbus Defence and Space

Dr. Kai Martius, secunet Security Networks AG

Prof. Dr. Johann Pongratz, TU Dortmund

REDAKTION & KOORDINATION

Benjamin Bellgrau, M. Sc., Referent für Öffentlichkeitsarbeit

Theresa Merkl, Kommunikationsdesignerin

ART DIRECTION

Tausendblauwerk, Agentur für Gestaltung
Michael Berwanger

www.tausendblauwerk.de

DRUCK

druckhaus köthen

https://koethen.de

REGULARIEN

1. Auflage, 550 Exemplare

Redaktionsschluss: Mai 2026

Titelabbildung: Adobe Stock / mankjon

ISBN: 978-3-98997-008-3 | ISSN: 2748-8780

Auch erschienen als elektronische Publikation
(ISBN: 978-3-98997-009-0 | ISSN: 2748-8799)
sowie in englischer Sprache
(ISBN: 978-3-98997-010-6 | ISSN: 2748-9485).

Disclaimer

Die im Jahresbericht enthaltenen Zahlen und Angaben wurden sorgfältig recherchiert und beziehen sich – sofern nicht anders vermerkt – auf den Stand zum 31. Dezember 2025. Trotz sorgfältiger Prüfung kann keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität übernommen werden. Irrtümer und nachträgliche Änderungen bleiben vorbehalten.


der Bundeswehr
Universität München
CODE
FI
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München