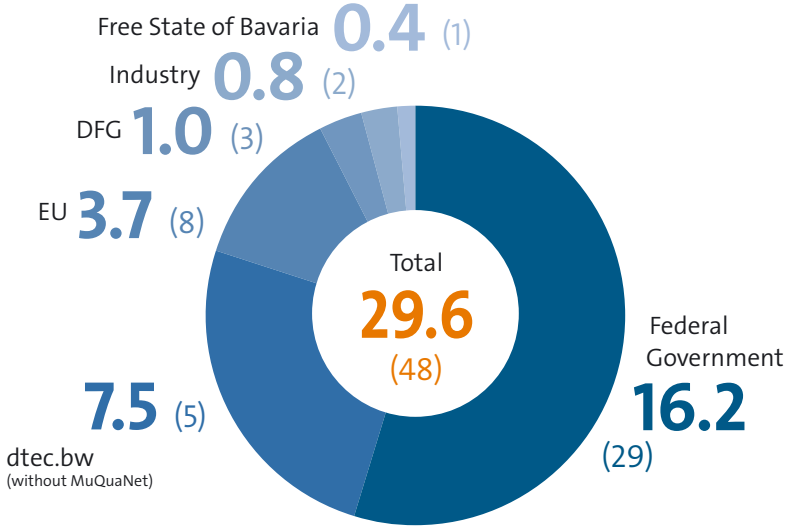

der Bundeswehr
Universität München
CODE
ANNUAL REPORT
2025
CODE
RI
Research Institute
Cyber Defence
Universität der Bundeswehr München

Project Funding

In 2025, a total of 48 projects financed by third-party funds were either processed or acquired. dtec.bw projects receive funding from the budget of the BMVg division.

Third-Party Funds*



* Numbers (rounded) in millions of euros, quantity of projects in parentheses.

dtec.bw Project**

MuQuaNet—The Munich Quantum Network

MuQuaNet
The Munich Quantum Network

Participating Professorships

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

** With participation of RI CODE and project start in 2020; not included in the third-party funds overview (left).

Internationality

RI CODE maintains a large international network.

Employees***

In 2025, CODE employees came from 19 countries.

Cooperation Partners***

In 2025, RI CODE cooperated with 79 partners in 27 countries.

Legend

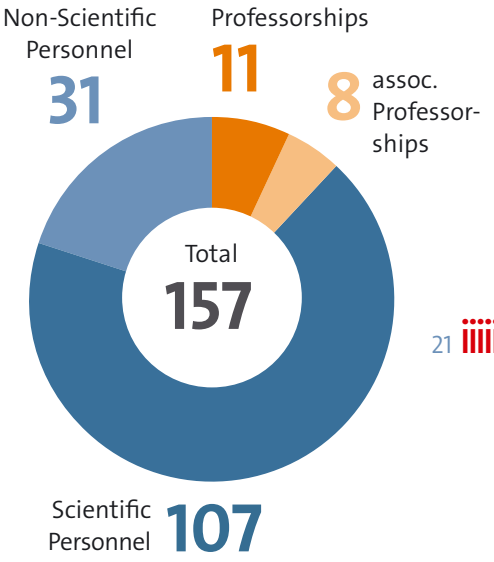
- Location of RI CODE
- 1 — Number of CODE employees from the country of origin
- 1 — Number of international cooperation partners in the respective country
- Countries with cooperation partners and employees

*** More information about contacts and cooperation partners can be found from p. 76 onwards.

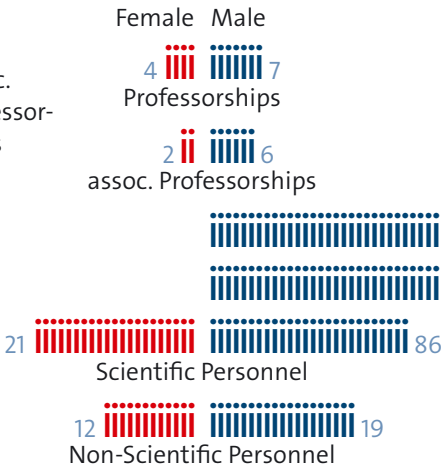
Staff Structure

**RI CODE had a total of 157 employees in 2025.
25 % of the staff were women.**

Employees



Gender Share



25 % **75 %**

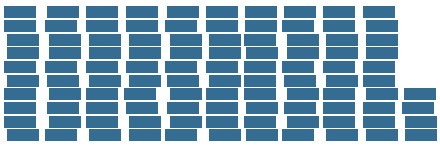
Research Work

Overview of doctorates and publications at RI CODE 2025

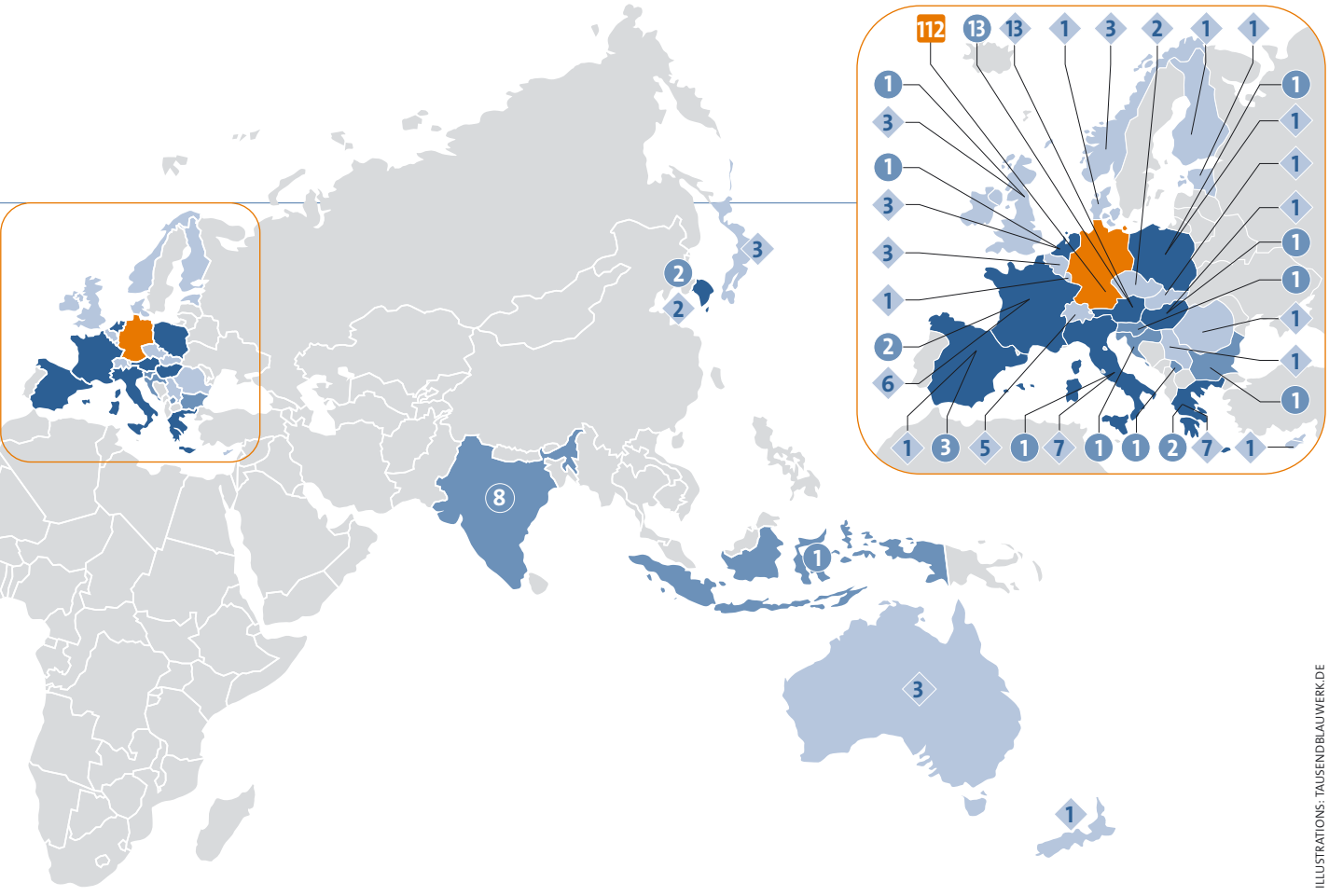
Doctorates

5

Publications



104



ILLUSTRATIONS: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
ANNUAL REPORT
2025

Research Institute
Cyber Defence
Universität der Bundeswehr München

Preface by the President

The ongoing digitalization and the increasing networking of critical systems pose growing challenges for society, the economy and state actors. Cybersecurity has become a central factor for resilience, agency and technological sovereignty. Given the ever-increasing cyberattacks on critical infrastructure, businesses and individuals, it is therefore essential to advance research in this area in a targeted and sustainable manner.

The Research Institute CODE makes a significant contribution on a national and international level, thereby sustainably strengthening the profile of the University of the Bundeswehr Munich as one of the leading institutions for security and resilience in technology and society.

2025 was characterized by the further development of central collaborations and successful research activities. The signing of a Memorandum of Understanding consolidated the long-standing cooperation between the UniBw M and Airbus. The aim of the partnership is to expand joint research projects, particularly in the areas of security, defence, aerospace and cybersecurity.

CODE has also made important progress in applied research. The MERLIN project in Carinthia presented a novel experimental blackout communication system that enables regional communication even in the event of failures of existing infrastructure. Through the launch of the EU-funded PiQASO project, CODE also further expanded international cooperation. Together with 24 partners, the institute is working on cryptographic foundations for quantum-safe communication in Europe.

In addition to research, the promotion of young talent and the commitment to diversity, equality and equal opportunities were another focus. At „Girls'Day 2025", 30 students received insights into study opportunities and current cybersecurity topics. In addition, a holiday workshop for girls lasting several days was held, which taught the basics of electronics, sensors and programming in a practical way. For their many years of commitment, Dr. Siegfried Brunner and Ulrike Nussel were awarded the Diversity Prize of the UniBw M.

Another highlight was the CODE Annual Conference 2025 with over 500 participants from science, the Bundeswehr, authorities and business, which further strengthened the professional exchange on cyber resilience.

The Research Institute CODE develops innovative solutions to tomorrow's challenges and strengthens our digital resilience. By its projects, it's helping to make Germany and the world safer. It I congratulate the entire institute on another successful year! Look forward to interesting insights into the world of cybersecurity!

With best wishes,

Prof. Dr. mont. Dr.-Ing. habil. Eva-Maria Kern, MBA
President of the University of the Bundeswehr Munich


Marcus Knüpfer, Michaela Geierhos and Wolfgang Hommel

Dear Readers,

In 2025, the Research Institute CODE once again proved to be a trusted partner for the Bundeswehr, government agencies and industry thanks to its profound technical expertise and numerous successful examples of transferring academic research into practical applications. We were particularly pleased to welcome several new research groups to our institute this year. In addition to Prof. Dr. Michael Hutter being appointed to the CODE Professorship of Embedded System Security in the Department of Computer Science, Prof. Dr.-Ing. Carmen Mas Machuca (Professor of Communication Networks in the Department of Electrical Power Systems and Information Technology), Prof. Dr.-Ing. Vladislav Nenchev (Professor of Embedded Systems in the Department of Electrical and Computer Engineering) and Prof. Dr. Christoph Peters (Professor of Information Systems with a focus on Digital Process Management in the Department of Economics and Management) joined CODE as associated members together with their research teams in the recent year, further broadening our range of expertise.

This year's focus areas, particularly artificial intelligence, are relevant to a variety of public outreach activities and the many application-oriented research projects featured in this annual report. For instance, a month-long AI event series in Munich attracted large audiences, while a university lecture on artificial intelligence inspired numerous young school kids.

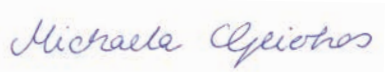
Developments like these are also being incorporated into the teaching process. The new artificial intelligence specialization track within the Master's degree program in computer science combines more than 50 courses into newly designed modules. These modules allow students to pursue either a technical specialization or an application-oriented focus. The courses are primarily taught by faculty members affiliated with the Research Institute CODE.

We are creating a strong technical and methodological nucleus with a broad range of application domains by bringing together the University of the Bundeswehr Munich's AI expertise across departmental boundaries within the Artificial Intelligence Competence Center (KompZ KI). We are working closely with our partners to enhance this capability.

Our partners also include representatives from other disciplines and organizations. In 2025, we hosted several cyber exercises, including Defence Cyber Marvel (DCM4) and Cyber Phoenix for the Bundeswehr Cyber Reserve. The OSINT Forum has also become a successful event, providing a platform for industry experts and OSINT specialists from the Bundeswehr and security authorities to exchange ideas.

We hope you enjoy the 2025 Annual Report and that our collaboration and shared activities will continue in the years ahead.

Prof. Dr. Wolfgang Hommel



Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Management of the Research Institute CODE

FIG.: UNIBW M; A. WAGENER FOTOGRAFIE

Contents

ABB.: ADOBE STOCK / ANDYAZIZ6

Highlights
From the Institute

Research
Portraits and Projects

Further Research Groups and Projects

Cooperations
Germany and the World

Young Science
Offers and Opportunities

Addendum
Publications and Activities

Organizational Structure

Categories

OUR MISSION STATEMENT

FIG.: ADOBE STOCK / GREENBUTTERFLY

The Research Institute CODE is a central scientific institution of the University of the Bundeswehr Munich. We use our expertise for the benefit of society and the Bundeswehr and contribute to making Germany a bit safer through innovations in the field of cyber/IT.

Three key areas are the focus of our activities:

- **Research and technology development**
- **Knowledge transfer and consulting for decision-makers**
- **Education and training**

We conduct both basic and applied research as well as technology development in the fields of cyber defense, smart data, and quantum technology. Our work focuses on the concrete and perspective benefits for society and the Bundeswehr. Due to our close ties with the Bundeswehr's CIDS (Cyber and Information Domain Service) military branch, we are in a unique position to develop solutions for current and future challenges in the CIDS domain through research in a secure environment.

Our goal is to research technical innovations and concepts for the protection of data, software, and systems in a holistic and interdisciplinary manner. In particular, we emphasize the development of application-oriented technologies and the acceptance of secure technologies by society. To this end, we work closely with the Bundeswehr, government agencies, research institutions, and industry so that our partners can transfer new research findings and technologies into practice in a way that adds value.

We are open to scientific discourse and pursue long-term cooperations. With the broad competencies of our professorships and research groups, we provide advice to decision-makers from the Bundeswehr and politics and promote knowledge transfer. Our scientific advisory board actively supports RI CODE in its strategic development with its technical expertise.

We offer an optimal framework for education and training. Our IT infrastructure allows research and training at the highest level. In teaching, we prepare students at the University of the Bundeswehr Munich for the challenges of their professional lives and provide practical training for members of the Bundeswehr and Cyber Reserve in our modern Cyber Range. Direct access to quantum computers enables us today to find innovative solutions for the challenges of tomorrow.

We stand by our responsibility and role model function to work together with our partners and, above all, the Bundeswehr to protect a free democratic society. Every day, we are working to make a significant contribution to protecting against the dangers in cyber and information space, and we are prepared to be measured against this. ■

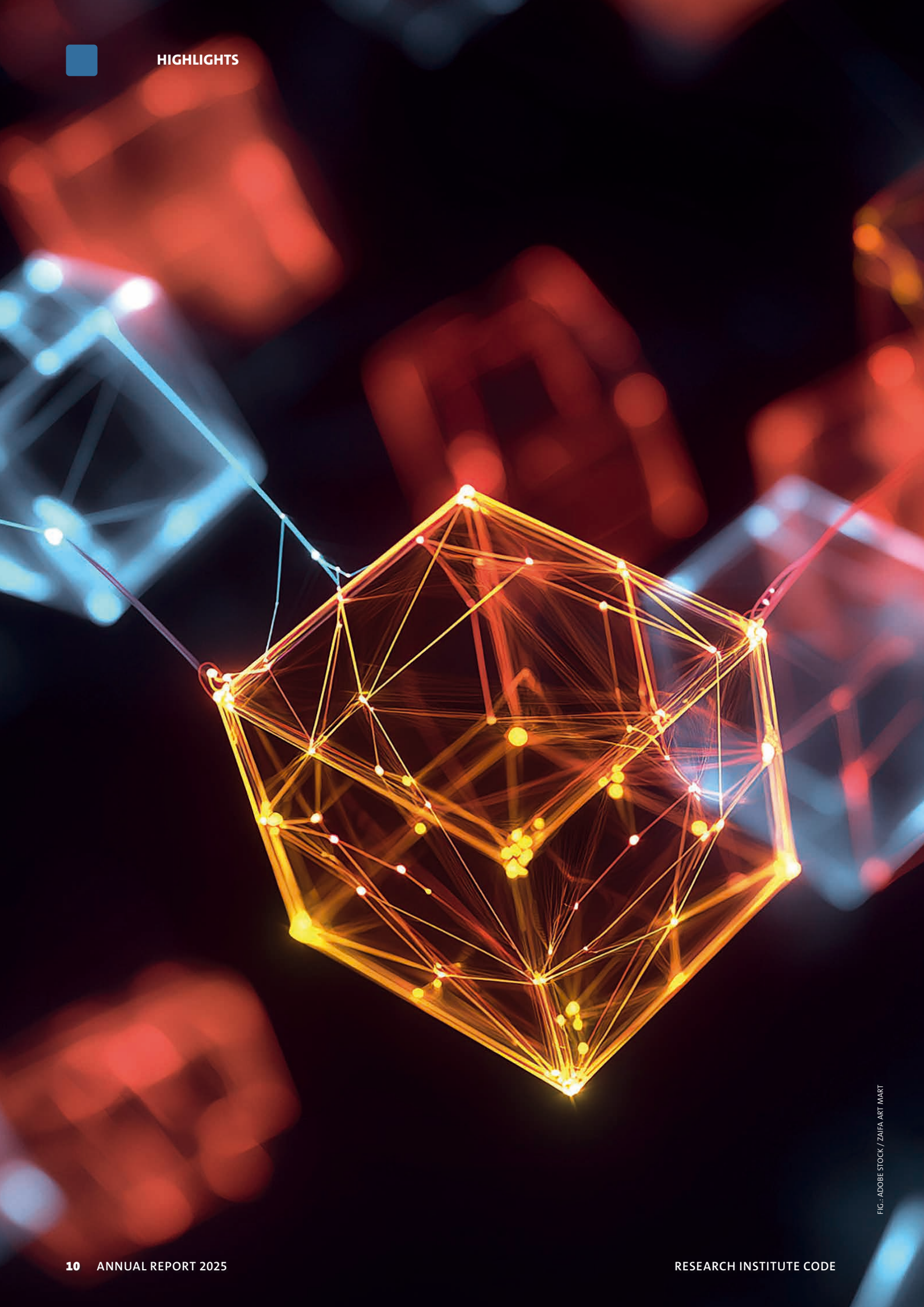


FIG.: ADOBE STOCK / ZAIFA ART MART

Highlights

From the Institute

Report on the CODE Annual Conference 2025

Tomorrow's Cyber Resilience – Proactive Rather Than Reactive

At the 2025 Annual Conference of the Research Institute Cyber Defence and Smart Data (CODE), well over 500 experts from academia, the Bundeswehr, government agencies, and industry came together once again to discuss current challenges in cyber resilience and jointly explore the future of cybersecurity.

BY BENJAMIN BELLGRAU

FIG.: RI CODE / ANGELIKA WAGENER FOTOGRAFIE (2)

AFTER THE WELCOME address by Prof. Dr. Karl-Heinz Renner, the Vice President of the University of the Bundeswehr Munich (UniBw M), Prof. Dr. Wolfgang Hommel, the Executive Director of CODE, provided participants with an overview of the institute's latest developments. Over the past twelve months, CODE has established three new specialist groups and launched several new research projects, particularly in the field of quantum technologies. Prof. Hommel also highlighted advances in artificial intelligence.

Beginning in January 2026, UniBw M will offer a new AI specialization track within its Master's degree program in Computer Science. Furthermore, the university is planning to establish an interdisciplinary AI Competence Center.

Keynote Speakers from Bundeswehr, Government, and Industry

In an era of increasingly complex and sophisticated cyber threats, it is crucial to not only respond to attacks, but also proactively counter them. Cyber resilience means designing systems that can withstand and quickly recover from attacks. This requires the coordinated interaction of technology, processes, and people. Cyberattacks, data breaches, and system failures are not isolated incidents; they are the new reality. This reality calls for a paradigm shift away from mere crisis management and toward strategic preparedness. This, in turn, requires a technological turning point. Innovative technologies must be rapidly identified and transitioned into operational use to ensure a combat-ready and future-oriented Bundeswehr. In his keynote address, Lieutenant General Michael Vetter, Director General for Cyber/Information Technology at the Federal Ministry of Defence (BMVg), emphasized that this will require greater risk tolerance.

This turning point is also increasingly affecting the scientific community. In a world shaped by global tensions, research institutions have become attractive, high-value targets for cyber adversaries. But how can the balance between academic freedom and security be maintained? Barbara Kluge, Ministerial Director at the Federal Ministry of the Interior, , addressed this question by emphasizing the role of the state, which "bears responsibility for protecting science and research in cyberspace as well," and called for swift and coordinated action.

Lieutenant General Michael Vetter during his keynote address.

In his keynote speech, General Major Jürgen Setzer addressed the topic of "(Cyber) Resilience Today and Tomorrow", emphasizing the importance of strategic foresight: "War is not only a competition of innovation, but also a driver of innovation." He noted that when introducing new technologies into the armed forces, resilience must be considered from the outset, and that personnel must be appropriately educated and trained.

Bernd Geisler, President of the Bavarian State Office for Information Security (LSI), then offered insights on "Cyber Resilience in Bavaria." He emphasized the importance of preparing for cyber incidents. In addition to preventive measures, he said that regular exercises are essential to determine how organizations should respond in a crisis in advance. To support this objective, the LSI and the Research Institute CODE will collaborate on developing and integrating real cyber incidents into cyber range training. The federal perspective was presented by the Federal Office for Information Security (BSI). Dr. Uwe Klapproth emphasized the importance of nationwide cooperation and used the LÜKEX exercise series to demonstrate how federal and state authorities prepare for emergency scenarios. "With smart resilience, shared responsibility, and decisive leadership, we can shape the race rather than merely react to it," Klapproth concluded.

Panel on the Cyber Resilience Act

Prof. Dr. Dennis-Kenji Kipker of the cyberintelligence. institute opened the second half of the afternoon with his presentation, "Why Security by Design Is a Topic for the Future!" He also provided a thematic introduction to the subsequent panel discussion. The panel, moderated by Lieutenant Colonel Katja Büchner of the Bundeswehr Centre for Digitalisation and Cyber and Information Domain Capability Development (ZDigBw), brought together Prof. Kipker, Andreas Witt (Sopra Steria SE), Sabine Griebsch (GovThings), Silvia Reischer (Swiss Institute for Global Affairs), and Andre Hinüber (Airbus Defence and Space). They discussed "The Cyber Resilience Act (CRA): Opportunity or Risk for Proactive Resilience Strategies?"

Addressing the question of whether the CRA is primarily restrictive or can serve as a catalyst for necessary developments, most panelists expressed support for the regulation, though they acknowledged several

Shaping the future of cybersecurity at the CODE Annual Conference 2025: Prof. Dennis-Kenji Kipker, Andre Hinüber, Sabine Griebsch, Silvia Reischer, Andreas Witt, and Lieutenant Colonel Katja Büchner (from left to right) discussed the European Union's Cyber Resilience Act (CRA).

Lieutenant General Michael Vetter (back row, fifth from left), Volker Eiseler (back row, right), both from the Federal Ministry of Defence (BMVg), and Prof. Wolfgang Hommel (back row, second from right) together with the finalists of the Cyber/IT Innovation Conference.

implementation challenges. The experts also viewed the CRA as an opportunity to draw attention to an important yet insufficiently focused issue that has existed for years. At the same time, concerns were raised about the potential for overregulation. The discussion then explored opportunities and policy priorities for strengthening Germany as a hub for security and technological innovation. Finally, the panelists outlined concrete implementation steps from their respective stakeholder perspectives.

Cyber/IT Innovation Conference

Another highlight of the conference was the Cyber/IT Innovation Conference, where innovative concepts with the potential to significantly improve cybersecurity capabilities were presented. Organized jointly with the Federal Ministry of Defence (BMVg), the competition operates under the principle of "Innovation Outside-In." A jury selected the seven most promising concepts from a total of 38 submissions for presentation. During seven-minute pitches, the finalists showcased their ideas to the expert audience at the CODE Annual Conference. The concepts ranged from AI-supported deception technologies and jam-resistant navigation based on multi-quantum sensor systems to the key technology LLLC (Lightweight Low-Latency Consensus) for trusted real-time PNT (Positioning, Navigation, and Timing) data.

The evening awards ceremony recognized the exceptional submissions to the competition and showcased the community's remarkable innovative potential. Justus Rischke and his Soron Systems team ultimately convinced the jury with their cooperative drone swarm navigation concept for environments where global satellite navigation systems, such as GPS, are unavailable or unreliable. Their proposal won first place in the innovation competition and was awarded € 15,000.

The Styx team, led by Jan Jeske, took second place with their concept "Tailored Analog AI Chips – Secure, Autonomous, Energy-Efficient, and Latency-Free," earning a prize of € 10,000. Martin Rick of Rick Location Solutions GmbH took third place with his idea, "Where GIS Meets EMS – Geospatial Intelligence for the Electromagnetic Spectrum", earning a prize of € 5,000. The teams that ranked fourth through seventh each received € 1,000.

Lieutenant General Michael Vetter presented the awards during the evening social event that concluded the first day of the CODE Annual Conference.

FIG.: RI CODE / ANGELIKA WAGENER FOTOGRAFIE (2)

Visitors to the CODE exhibition booth gained first-hand insights into the institute's current research activities.

Proactive Risk Management

Prof. Dr. Michaela Geierhos, Technical Director of the Research Institute CODE, opened the second day of the CODE Annual Conference 2025. In her opening remarks, Geierhos stated, "Tomorrow's cyber resilience requires a shift in both thinking and action—a transition from a 'firefighting mode' to proactive risk management". She concluded with the appeal, "Let us anticipate challenges together rather than merely respond to them," before handing the floor over to Major General Armin Fleischmann of the Cyber and Information Domain Service Command.

In his keynote address, "Cyber Resilience – Only Those Who Plan Remain Resilient," the Commander Support Cyber and Information Domain Service (CIR) and Director for CIR Planning and Bundeswehr Digitalization illustrated the concept of resilience through current examples and outlined possible solutions. His central message was clear: Resilience requires planning for adverse events before they occur.

Two professors from the Research Institute CODE then shared insights into their current research activities. Prof. Dr.-Ing. Mark Manulis, Professor for Privacy, presented recent cryptographic approaches to encryption and authentication aimed at improving security in cloud environments. Maximilian Moll, Junior Professor of Operations Research – Prescriptive Analytics, introduced his research on quantum machine learning. The mathematician gave an engaging presentation that made this highly abstract and complex field accessible to the audience while also highlighting the current challenges and uncertainties surrounding this emerging area of research.

After the coffee break, the focus remained on quantum computing. In his presentation, "Quantum Safe and Cyber Resilience – Achieving Success Through Their Interaction," Dr. Silvio Dragone of IBM Research discussed the risks posed by quantum computers. These systems have the potential to break conventional encryption algorithms in a short amount of time. Dr. Dragone emphasized the importance of implementing post-quantum cryptographic standards to ensure long-term cybersecurity and resilience.

Cybersecurity and digitalization are key factors to a successful future. Recognizing this early on, the European Union launched the Horizon Europe and Digital Europe programs to support cybersecurity research

FIG.: RI CODE / ANGELIKA WAGENER FOTOGRAFIE (2)

and innovation, as well as the development, deployment, and practical application of digital capabilities and innovative technologies. In his presentation, "Europe? Secure, of Course! – The Role of the National Cybersecurity Coordination Centre (NCC)," Dr. Christian Fischer of the DLR Projektträger offered insights into the NCC's activities, networks, and extensive support services. The Research Institute CODE is also a member of the NCC.

On the second day of the CODE Annual Conference, Dr. Michael Kissner of Akhetonics GmbH was among the speakers. In his presentation, "Chip Security & Resilient Semiconductor Supply Chains – Can You Prevent Hardware Backdoors?," the winner of the 2023 Cyber/IT Innovation Conference addressed the risks posed by compromised hardware in security-critical systems. He demonstrated how hardware backdoors could be deliberately embedded in microchips manufactured outside Europe without detection.

The lecture series concluded with a presentation by Prof. Dr. Bernhard M. Hämmerli, Professor of Information and Network Security at Lucerne University of Applied Sciences and Arts and the Norwegian University of Science and Technology (NTNU). With over three decades of experience in research, teaching, and consulting, Prof. Hämmerli is considered a pioneer in of European cybersecurity research. In his presentation, "Resilience – Optimizing Pre- and Post-Loss Measures for an Evolving Threat Landscape," Hämmerli began by outlining the fundamental attack vectors in information technology. He then presented possible courses of action and decision-making pathways in the event of a cyberattack. Drawing on recent surveys of Swiss companies, he also illustrated how organizations are preparing for such incidents and strengthening their resilience against future threats.

The afternoon workshops on the second day of the conference covered a broad spectrum of topics, ranging from quantum technologies and trustworthy AI to serious games.

More information on the CODE Annual Conference

www.unibw.de/code-en/events/annual-conference

www.youtube.com/@FI_CODE

code@unibw.de

Tackling Cybersecurity Issues as a Team!

After two intensive days filled with inspiring presentations, lively discussions, and valuable exchanges, the CODE Annual Conference came to a close. Guided by the theme "Tomorrow's Cyber Resilience – Proactive Rather Than Reactive," participants explored the future of cybersecurity together.

"Lastly, we would like to emphasize the valuable networking and exchange opportunities that make this conference so distinctive. Conversations during breaks, discussions following presentations, and informal meetings have demonstrated the value of personal interaction is for our work," said Prof. Dr. Michaela Geierhos. "Whether we're discussing the integration of quantum technologies into cybersecurity or trustworthy artificial intelligence, the diversity of workshop topics reflects the complexity and dynamism of our field," she added.

In closing, Prof. Geierhos thanked everyone who contributed to the conference's success, from the speakers and members of the expert jury to the sponsors and the many individuals working behind the scenes. She also announced that the next CODE Annual Conference will take place on July 14 and 15, 2026. Once again, experts from across academia, government, the armed forces, and industry will come together to discuss cybersecurity challenges and develop solutions for a resilient digital future. ■

Workshop Report from the CODE Annual Conference 2025

AI and Leadership

In the international workshop, forecasts for the short-term and long-term development of innovative AI technology were characterized and its potential in the area of forward-looking management processes was identified. In addition, concrete recommendations for action were derived at the end. The workshop focused on generative AI, reliability, and quality assurance in relation to complex leadership processes, as well as on the specific aspect of characterizing accountability in the "human-in-the-loop" process.

BY STEFAN PICKL

The discussion began with the fluctuating output quality when using AI processes and the role of humans in the "human-in-the-loop" process. How can and will bias, fairness, transparency, as well as data and model distortions systematically influence decisions in the future? This limits explainability and traceability, especially in the area of generative AI. Governance and compliance, along with fragmented regulatory landscapes (e.g., AI Act, industry guidelines) are increasingly encountering heterogeneous toolchains. Without clear policies and objectives, there is a risk of shadow AI, data silos, and reputational risks. Participants agreed that data protection and intellectual property, the use of sensitive data, training leaks, IP issues with generated content, and supply chain issues (third-party models/APIs) will remain challenging in this context, both legally and technically.

In the second part of the workshop, that was moderated by Prof. Dr. Stefan Pickl, an intensive panel discussion was held to identify individual potentials and recommendations for action in these core areas: If people are to remain "in the loop," roles, approval steps, and liability must be clearly defined—especially for security-critical or regulated decisions within management processes. Bias, fairness, transparency, data and model distortions can also systematically disadvantage decisions.

The following potentials were identified:

- **Better Decisions through Augmentation**
  AI expands perception and options (scenario analysis, early risk warning, real-time analyses and optimization, hypothesis generation), while humans can contribute context, values, and judgment.
- **Productivity and Quality Gains**
  Automated synthesis, drafting, summarization, and assistant functions accelerate complex knowledge work and improve the quality of repetitive or data-intensive tasks.
- **Democratization of Analytics**
  Natural language interfaces and GenKI lower the barriers to entry for complex analyses ("self-service BI++") – particularly helpful for managers who need viable insights quickly.
- **Organizational Learning**
  Feedback loops in human-in-the-loop processes create dynamic knowledge bases and better decision-making heuristics.

The panel discussion and subsequent statements focused primarily on the systematization of capability development, in which CODE could play a central role. A forward-looking operating model and living lab for "human-in-the-loop" were also proposed.

At the end, there was an open discussion on how AI governance and policies can be established in the long term. The aspects of "augmentation instead of substitution," "transparent benefit/risk narratives," "employee participation," and the "characterization and analysis of measurable trust indicators" could serve as a model here.

These are topics that CODE is working on in an international context. The exchange is to be continued in 2026. ■

Led by Prof. Dr. Stefan Pickl (m.), Juniorprof. Dr. Maximilian Moll (l.) and Prof. Dr. Bernhard Hämmerli, member of the Swiss Academy of Engineering Sciences, (r.) discussed with the workshop participants.

FIG.: RI CODE / ANGELIKA WAGENER FOTOGRAFIE (2)

The first IBM Quantum System Two in Europe, at the IBM-Euskadi Quantum Computational Center in San Sebastián, Spain.

Quantum Technologies

From Fundamental Research to Quantum Applications

Quantum technologies are considered among the most promising and potentially disruptive developments of our time. They promise far-reaching impacts on defense, science, and industry — ranging from novel sensors and secure communication methods to powerful quantum computers.

BY SABINE TORNOW

IN TERMS OF CONTENT, four central capability areas can be distinguished within the field of quantum technologies: navigation and timekeeping, cryptography, sensing, and computing. In the area of navigation and timing, quantum sensors and highly precise atomic clocks enable new forms of GPS-independent positioning and time determination, which can enhance mission security in complex operational environments. In the field of electromagnetic sensing and imaging, quantum-based detectors open up possibilities for more robust and precise data acquisition. In computing, the focus is on long-term potential, such as materials and chemistry simulation, the optimization of complex logistical processes, the analysis of quantum data, and improvements in AI models. It should be emphasized that many of these concepts have not yet been demonstrated in detail — nevertheless, their disruptive potential remains high.

From a military perspective, the maturity level of these technologies varies considerably. Large fault-tolerant quantum computers are still far from practical operational readiness. Quantum sensors and atomic clocks, by contrast, are at an intermediate level of maturity and appear significantly closer to possible integration.

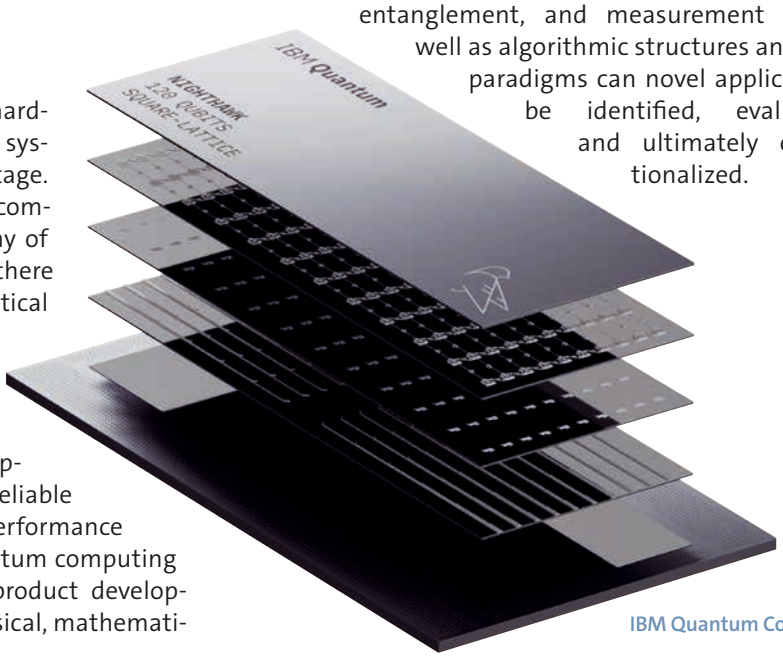
The Role of Fundamental Research

Despite considerable progress in hardware development, many quantum systems are still at an experimental stage. Powerful, fault-tolerant quantum computers do not yet exist, and for many of the applications under discussion, there is still no robust evidence of a practical advantage over classical methods.

This is precisely where fundamental research comes in. Without it, neither new and realistic fields of application can be identified, nor can reliable statements be made about actual performance gains. Fundamental research in quantum computing is not concerned with short-term product development, but with the fundamental physical, mathematical, and information-theoretical principles of quantum information processing. It investigates the properties of qubits, the limits of coherence and fault tolerance, the structure of quantum algorithms, and the conditions under which a quantum-mechanical advantage is possible at all.

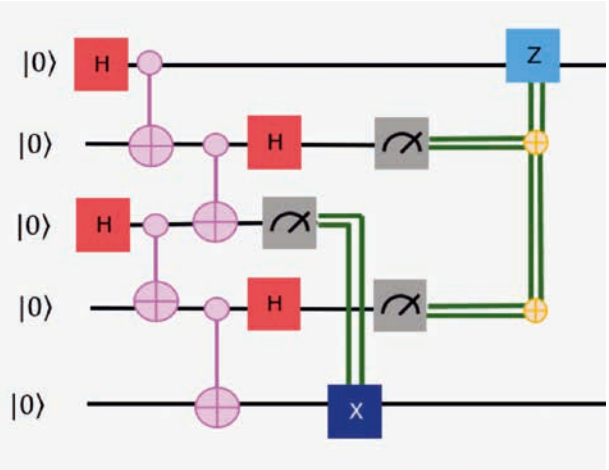
Only through this deep understanding can viable strategies for scalable systems be developed and potential applications critically assessed. Before quantum computers can solve practical problems in cryptography, materials research, or optimization, fundamental questions concerning stability, scalability, error correction, and algorithmic advantage must be clarified. Fundamental research is therefore not a preliminary stage of application, but its prerequisite. It creates the scientific foundation on which future technological breakthroughs can become possible.

New qubit materials, scalable architectures, innovative algorithms, and the analysis of fundamental information limits are necessary. In many cases, applications still have to be discovered; they do not automatically arise from existing hardware. Only through a deep understanding of physical phenomena — interference, entanglement, and measurement — as well as algorithmic structures and new paradigms can novel applications be identified, evaluated, and ultimately operationalized.



IBM Quantum Computer

BOTH FIG.: IBM



Dynamic circuits with intermediate measurement and reset.

In the field of quantum algorithmics, the central challenge today is not only to formulate theoretically interesting methods, but also to implement them under realistic conditions on error-prone quantum hardware. In this context, fundamental research means developing new computational paradigms that do not treat physical dynamics, noise, measurement processes, and limited coherence times as disruptive factors, but instead systematically integrate them into the algorithmic structure.

Quantum walks represent a quantum-mechanical generalization of classical random walks on graphs. While classical processes exhibit diffusive spreading, in the quantum case interference gives rise to non-classical dynamics that, under suitable conditions, can lead to speedups.

A central algorithmic approach is the investigation of the first hitting time: this analyzes how long it takes on average until a specific target state is detected for the first time, and how this time depends on the spectral structure of the underlying graph or Hamiltonian.

Unlike in the classical case, the definition of a "hit" is not trivial in the quantum case, since every measurement changes the state. In our research, such processes are investigated both theoretically and experimentally on programmable quantum hardware. By implementing mid-circuit measurements, first-hitting statistics can be extracted directly from real measurement data. [1]

In parallel, we are investigating **quantum reservoir computing** as a particularly hardware-oriented approach to machine learning and time-series forecasting. The basic principle is to use the natural dynamics of a quantum system as a nonlinear reservoir: input data are fed into the system, the internal dynamics transform them into a high-dimensional state space, and only the readout unit is trained.

In contrast to variational quantum algorithms or parametric quantum networks, the entire system therefore does not need to be optimized. This significantly reduces the training effort while still allowing complex temporal patterns to be processed. This approach is particularly promising because it enables powerful computations already on currently available, error-prone, quantum hardware.

A key research result is the development of a protocol for efficient feedback processing in quantum reservoirs. Previous approaches were either very time-consuming or did not allow feedback loops, which limited the processing of temporal correlations.

Our new protocol integrates feedback connections directly into the continuous quantum process: by using dynamic circuits with mid-circuit measurements and immediate feedforward, the system can process information within the coherence time of a qubit and "remember" past inputs without interrupting the computation.

This architecture significantly increases the reservoir's memory capacity and predictive power while maintaining high processing speed. The ability to implement fast feedback loops is also of central importance for future quantum error-correction protocols. [2]

A fundamentally new computational paradigm emerges from transferring **stochastic resetting** into the quantum world. In classical statistical physics and computer science, **resetting** is an established principle: in diffusive or randomized search processes, an optimal reset rate can make an otherwise divergent mean first-passage time finite — a concept that is also routinely used in randomized algorithms and Monte Carlo methods.

In quantum mechanics, this principle is fundamentally extended, since coherence, entanglement, and measurement backaction add a new dimension: every reset acts as a measurement and preparation step that changes the quantum state. The interplay between unitary dynamics and targeted nonunitary interventions thus enables non-classical speedups that have no counterpart in classical resetting.

In addition, another part of our research is devoted to the fundamental control of **quantum many-body systems** far from thermal equilibrium. In an experimental study on programmable quantum hardware, we were able to show that targeted stochastic resets

FIG.: IBM / SIMONE CANTORI; IBM

can generate stable and controlled states in interacting qubit systems.

For this purpose, a theoretical model was developed that precisely describes measurement processes and nonunitary dynamics; this model was experimentally validated. The results establish stochastic resetting as a new basic method for deliberately controlling complex quantum dynamics, stabilizing metastable regimes, and providing controlled states for algorithmic applications. [3]

Conclusion

Overall, it becomes clear that fundamental research in quantum algorithmics today goes far beyond the construction of idealized, deep circuits. It includes the development of new computational models, the systematic integration of measurement and feedback, the analysis of time-to-event structures in the quantum domain, and the use of nonequilibrium dynamics as an algorithmic resource.

The three research directions presented here — quantum-walk-based first-hitting-time analysis, quantum reservoir computing with integrated feedback, and stochastic resetting — illustrate how fundamental theory, experimental hardware, and algorithmic innovation can be brought together.

These works not only define new pathways toward applications but also make a fundamental contribution to understanding what computation means in the quantum-mechanical sense and under which physical conditions a robust advantage can be realized. ■

PUBLICATIONS

Literature for 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).

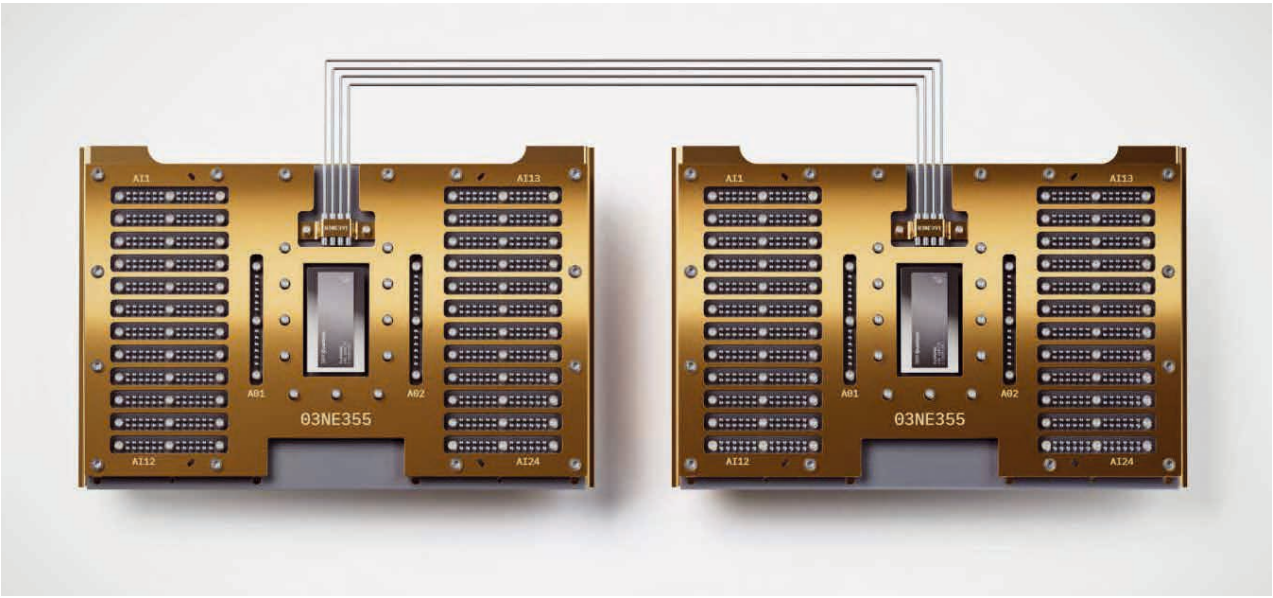
YIN, R., WANG, Q., TORNOW, S., BARKAI, E.: Restart uncertainty relation for monitored quantum dynamics. PNAS 122 (1), e2402912121.

Literature for 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).

Literature for 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.



Modular Quantum Computing.

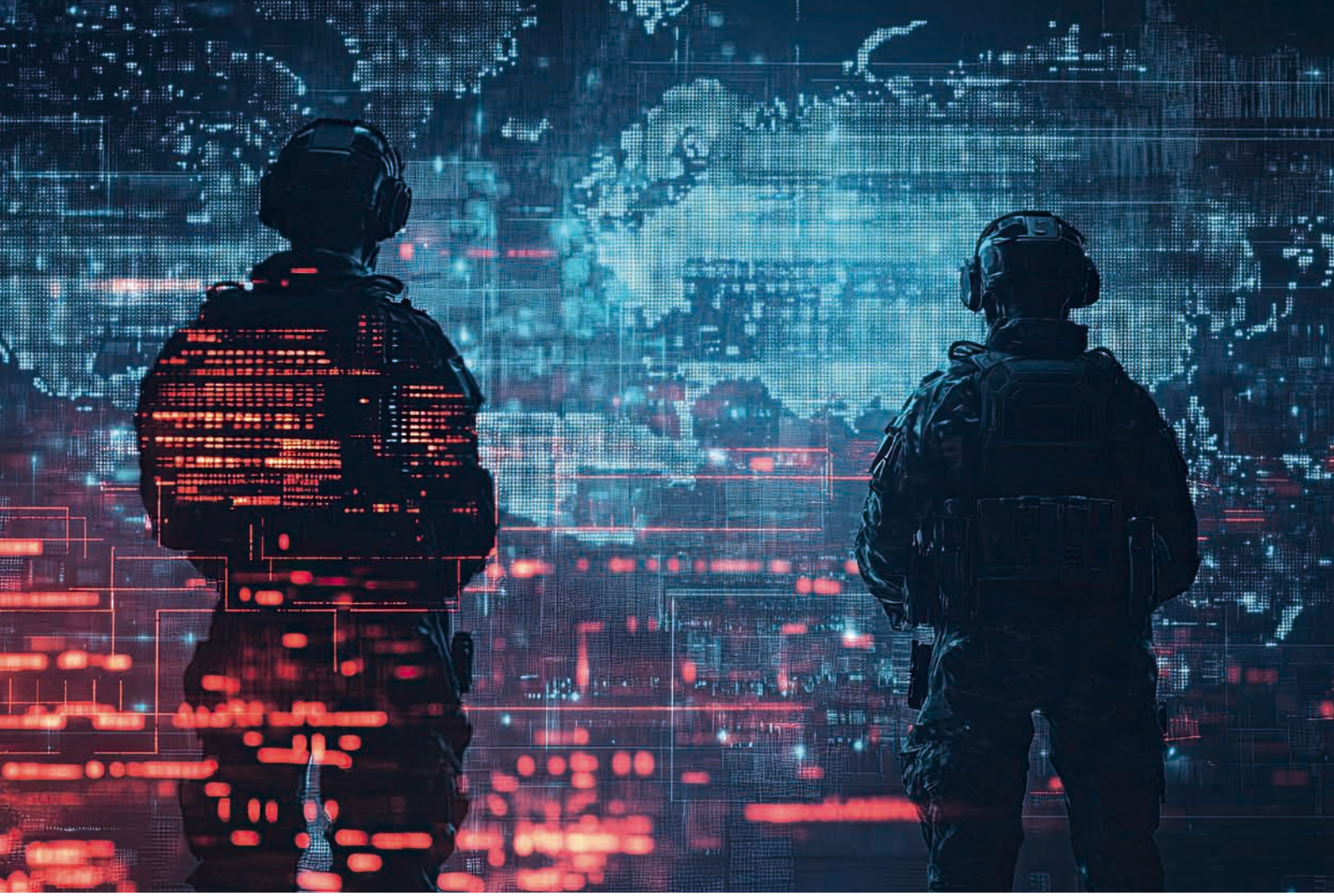


FIG.: ADOBE STOCK / KAIHKOIMAGES

National Cybersecurity Coordination Centre Germany

Cybersecurity Research Needs in the German Defence Sector

Common investigations to strengthen cybersecurity and ensuring Germany's digital sovereignty

BY CORINNA SCHMITT

CYBERSECURITY INVESTIGATIONS are of critical importance in the current digital landscape, particularly for the German defence sector, which faces increasingly sophisticated cyber threats from both state and non-state actors. As modern warfare extends into cyberspace, attacks targeting critical infrastructure, military networks, and defence technologies directly threaten national security and operational readiness. Timely and thorough cyber investigations are essential for identifying vulnerabilities, attributing attacks, and implementing effective countermeasures, thereby ensuring Germany's digital sovereignty.

Cybersecurity investigations are critically important in today's digital landscape, especially for the German defence sector, which faces increasingly sophisticated cyber threats from both state and non-state actors. As modern warfare expands into cyberspace, attacks

targeting critical infrastructure, military networks, and defence-related technologies pose direct threats to national security and operational readiness. Timely and thorough cyber investigations enable the identification of vulnerabilities, attribution of attacks, and implementation of effective countermeasures - ensuring that Germany can defend not only its physical borders but also its digital sovereignty. Equally essential is the adoption of a dual-use approach that bridges civilian and military capabilities. Civilian sectors often lead in innovation, speed, and adaptability, while the military provides robust security protocols, strategic intelligence, and resource depth. By integrating these strengths, Germany can create a resilient, agile, and future-proof cyber defence posture. Collaboration between civilian research institutions, private tech firms, and military agencies fosters a holistic and unified cybersecurity strategy, vital for securing the nation in an era where the line between peace and conflict is increasingly blurred by digital operations.

Thus, RI CODE as part of the National Cybersecurity Coordination Center Germany investigated over 30 months, which topics are of interest in the German defence. The results are part of the related project NCC-DE funded under the EU-Digital Europe Programme (DIGITAL) with No. 101126787. Stakeholders from academia, research institutes, SMEs, and industries across various application areas like automotive, health, building, aeronautics, space, logistics, and critical infrastructures overwhelmingly stated that a sharp distinction between civil and military areas in cybersecurity and investigations no longer makes sense and can even be obstructive. They clearly prefer the dual-use approach, seeing clear benefits. This integration leverages civilian innovation, speed, and adaptability alongside military security protocols, strategic intelligence, and resource depth to create a resilient, agile, and future-proof cyber defence posture. Collaboration between civilian research institutions, private tech firms, and military agencies is considered vital for a holistic and unified cybersecurity strategy. Summarizing the taken discussions, foreseen investigations are required in concrete applications areas – Vehicle-to-Everything (V2X), Zero Trust Security, Endpoint Security, Satellite Communications (SatCom), and Unmanned Aerial Vehicles (UAV) – as well as toward a global strategic focusing on a robust cybersecurity strategy and operational technology (OT) security. Manifold subtopics and area were mentioned looking on cryptographic, communication, network infrastructure, cloud services, and data exchange as well as on trainings, incident responds developments, and standardization. ■

PD Dr. Corinna Schmitt
corinna.schmitt@unibw.de
www.nkcs.bund.de/en

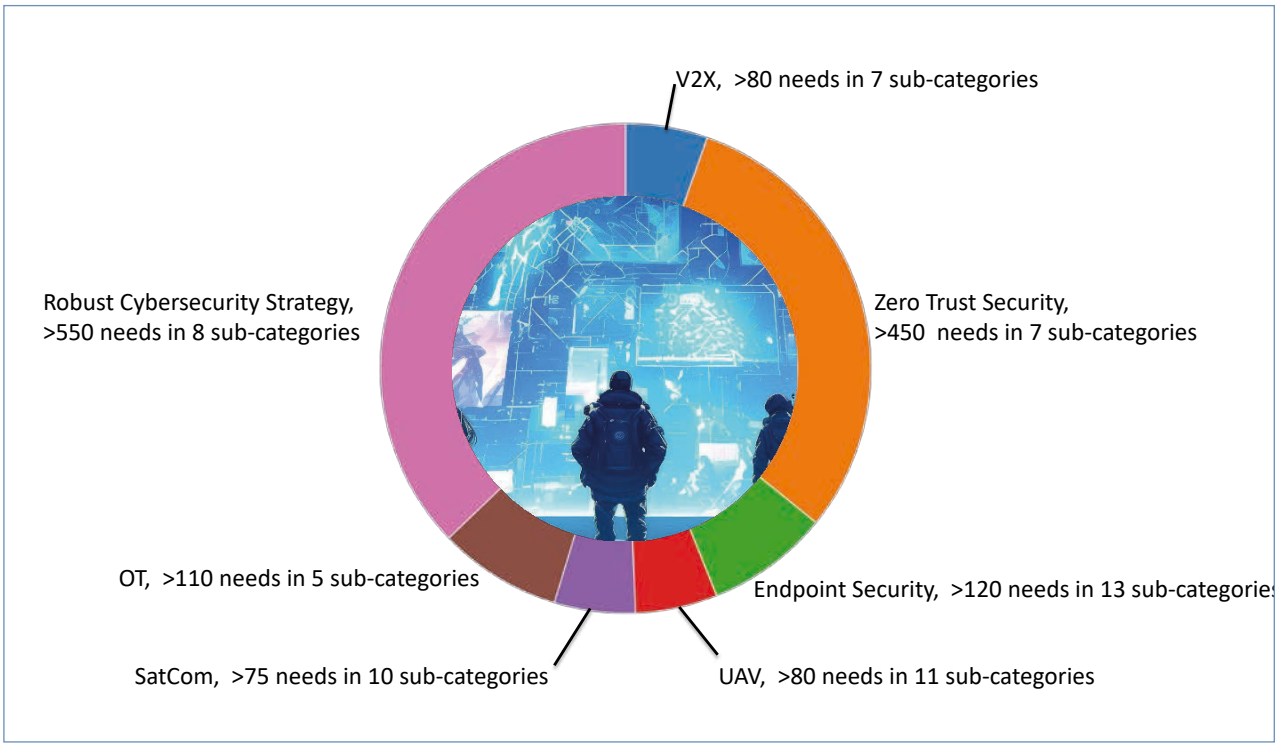


FIG.: RI CODE / C. SCHMITT; PICTURE: ADOBE STOCK / YANLONG

Schematic split of research needs in the German defence sector.

Group photo of the participants at DigiTwin 2025.

Report on DigiTwin Conference 2025 in Garmisch-Partenkirchen

Digital Twins Optimizing the World

The fifth international conference on the topic of "Digital Twin" took place in Garmisch-Partenkirchen from October 14th to 18th, 2025. Leading researchers and industry partners gathered under the special theme "Digital Twin Optimizing the World", to exchange new results, discuss boundaries and create a high-level platform for international exchange.

BY STEFAN PICKL

DIGITAL TWINS HAVE evolved from a conceptual framework into a mature research and engineering paradigm that delivers measurable scientific and practical value across many domains, particularly in cyber-physical systems. By aligning models, data, and control in a closed loop, they enhance reliability and quality, shorten lead times, reduce costs and energy use, and strengthen especially safety & security and resilience. In this context, the fifth Digital Twin International Conference took place from October 14 to 18, 2025, in Garmisch-Partenkirchen, Germany. Under the special theme "Digital Twins Optimizing the World,", the conference convened leading researchers and industrial partners to share new results, discuss frontiers, and build a high-level platform for international exchange that advances innovation in digital twin science and engineering. The hybrid program comprised three venues for in-person participation together with 21 online venues, delivered 226 academic presentations, and attracted more than 1,200 registrants from over 20 countries.

Digital Twins Optimizing Smart Cities

Cities are complex and interdependent systems shaped by human behavior and policy and digital twins synchronize sensing, modeling, and control across energy, transport, water, and buildings to improve public services through real-time analyses and data-driven optimization. By integrating demand, condition, and environmental data into unified models, twins enable accurate forecasts and adaptive control for traffic systems, building automation, and distributed energy, while reliability is enhanced through anomaly detection and corrective action.

Urban planning benefits from detailed scenario analyses that test policies for resilience, equity, and emissions, and during emergencies, digital twins guide evacuation and resource allocation. Building-level models support model-based control, while districts coordinate to balance load and integrate renewables, and citizens gain transparency as performance and decisions become data-driven and traceable. With these digital capabilities, cities can reduce emissions and delays while improving safety & security and service equity.

FIG.: UNIBW M / S. PICKL

In addition, the following other topics were discussed during the conference:

- Digital twins optimizing healthcare
- Digital twins optimizing aviation management processes
- Digital twins optimizing transportation and logistics
- Digital twins optimizing cyber-physical systems

Real-time Optimization and Safety Constraints

The common central challenge is the creation of real-time, and scalable digital twin loops that perform reliably under resource constraints and safety limits. Research priorities include robust data assimilation from sparse or delayed inputs, multiscale modeling with validated error bounds, and hierarchical control with explicit guarantees on latency and safety. Runtime metrics should quantify latency, throughput, accuracy, and resource usage, and progress requires realistic datasets, open platforms, and interactive testbeds (Living Labs) that enable reproducible evaluation and data-driven optimization.

Standards, Ethics, and Governance

As digital twins influence outcomes in the physical world, standards and governance must also ensure transparency and accountability. Common metadata and formats should enable the transfer of models across environments, while ethical legitimation requires bias detection, the exposure of uncertainty, and clear limits of validity. Governance should define data responsibility, model change control, and audit practices, while certification demands rigorous testing regimes and reporting structures that reflect operational expertise.

Keynote speakers included Juniorprof. Dr. Maximilian Moll, Prof. Dr. Bernhard Hämmerli (Swiss Academy of Technical Science), and Honorary Professor General (ret.) Dr. Dr. Dieter Budde. Juniorprof. Dr. Moll received the Best Presentation Award.

The Chair of the Conference was Prof. Dr. Stefan Pickl. HOLM and Research Center RISK were partners of the conference, which took place in Germany for the first time. The next DigiTwin Conference will take place in August 2026 at the University of Oxford. ■

MERLIN

Blackout-proof Communications Infrastructure for Crisis Situations

Regional disasters such as extreme weather events often go hand in hand with the destruction of public infrastructure. When electricity, mobile phone, and internet access fail in towns cut off from the outside world for days on end, it becomes extremely difficult for emergency services to assess the situation due to the lack of direct communication with those affected. MERLIN, a research prototype for self-sufficient emergency communication via LoRa radio, has been put into operation in the Carinthian municipality of Neuhaus.

BY MARIO SILACI

IN THE SUMMER of 2023, prolonged heavy rainfall and landslides destroyed several roads and bridges in the municipality of Neuhaus. Due to the low mountain range location in the border area with Slovenia and heavy forestation, entire districts and numerous smaller settlements could no longer be reached by emergency services in a timely manner without putting themselves at risk. Due to inherently suboptimal mobile phone coverage in the affected area and destroyed telephone lines, direct contact was not possible, for example, to focus relief efforts on acute life-threatening emergencies.

Through joint contacts in the Austrian Armed Forces, which supported crisis management in 2023, a cooperation was established with the dtec.bw project ROLORAN, carried out at RI CODE, which investigates civil and military applications of LoRa radio technology in technically challenging environments. In September 2025, MERLIN ("Messaging with Regional LoRa Infrastructure"), the second generation of a research prototype, entered long-term testing in ten localities in the Neuhaus municipal area.

Communication Between the Population and the Crisis Management Team

MERLIN enables text-based messaging between a crisis management team set up by the municipality and those affected, as well as mobile emergency ser-

FIG.: RI CODE / DR. MICHAEL GRABATIN (2)

Demonstration of MERLIN during an expert workshop.

Presentation of MERLIN at the press conference in Neuhaus.

vices. In Neuhaus, ten stationary MERLIN bases set up a radio mesh network covering the entire municipal area. The MERLIN bases are converted telephone booths equipped with electronic components developed as part of the project and our own software. Integrated E-Ink monitors display incoming messages and, together with a connected keyboard, enable the guided sending of emergency alerts and notifications.

All MERLIN bases are powered by photovoltaic elements and have a battery buffer that can bridge several weeks without significant sunlight.

The mobile MERLIN messengers for households and emergency services are equipped with comparable functionality. They can be operated continuously for around two weeks using a standard power bank. With a touchscreen, a small keyboard, and smartphone size, they allow messages to be sent and received within range of the MERLIN bases and can also be used as mobile repeaters to extend the area covered by LoRa radio.

All messages sent by MERLIN bases and MERLIN messengers are received by crisis management software. With MERLIN Messenger connected to a computer, the software enables correspondence between the crisis management team and MERLIN bases/messengers, as well as management of the LoRa radio network. Similar to email programs, messages can be sent, received, edited, and annotated to communicate with citizens or emergency services and coordinate relief efforts. Periodically updated overview pages on the status of the entire network provide a quick assessment of the functionality of the infrastructure and offer tools for remote maintenance.

Practicing for Emergencies

At the end of September 2025, the MERLIN infrastructure was presented in Neuhaus at public information evenings, expert panels, and a press conference, receiving positive feedback from all participants. Since October 2025, regular crisis exercises have been conducted to establish routines and ensure that MERLIN is ready for use in an emergency. The results of these practical tests under various weather conditions and over a longer period of time are being incorporated into the further improvement of the prototype. Among other things, the integration of decentralized sensor data is planned for 2026 to further improve the crisis management team's overview of the situation.

MERLIN software for the crisis management team.

MERLIN Messenger mobile device

We would like to thank the municipality of Neuhaus and all local volunteers for their support in the long-term test operation! ■

FIG.: RI CODE / DR. MICHAEL GRABATIN (3)

FIG.: UNIBW M

Honor for Stefan Pickl

Admittance to the Club of Rome

On September 18, 2025, Stefan Pickl, Professor for Operations Research at the University of the Bundeswehr Munich, was appointed as member of the international Club of Rome.

PICKL WAS AWARDED this honorary membership for his services to the scientific analysis and modeling of crisis and conflict scenarios, as well as for the innovative solutions he has developed: "He is a systems thinker with an ability for establishing connections between different disciplines—from electrical engineering and philosophy to game theory and peacebuilding," wrote the Club of Rome on his appointment.

Furthermore, the organization recognized his broad social and internationally networked commitment to civil protection and the protection of critical infrastructure, for example as a member of the Scientific Advisory Board of the Federal Office for Civil Protection and Disaster Relief (BBK), as a member of the German National Academy of Technology (acatech), and as Vice President of the German Committee for Disaster Reduction (DKKV). Prof. Pickl is also a founding member of the RISK Research Center at the UniBw M.

As one of the first scientists worldwide, Stefan Pickl developed a mathematical model for modeling, analyzing, and optimizing worldwide CO2 certificate trading. These studies are still highly relevant today and also influence general resource conflict scenarios and crisis predictions. Prof. Pickl works with Ernst Ulrich von Weizsäcker (former co-president of the Club of Rome) and considers the biochemist and systems researcher Frederic Vester (1925 – 2003) one of his role models. He is particularly pleased that Vester himself was a professor at the UniBw M, thus continuing the tradition of "The Art of Interconnected Thinking" (a term coined by Vester) in Munich. ■

FIG.: ADOBE STOCK / MANKJON

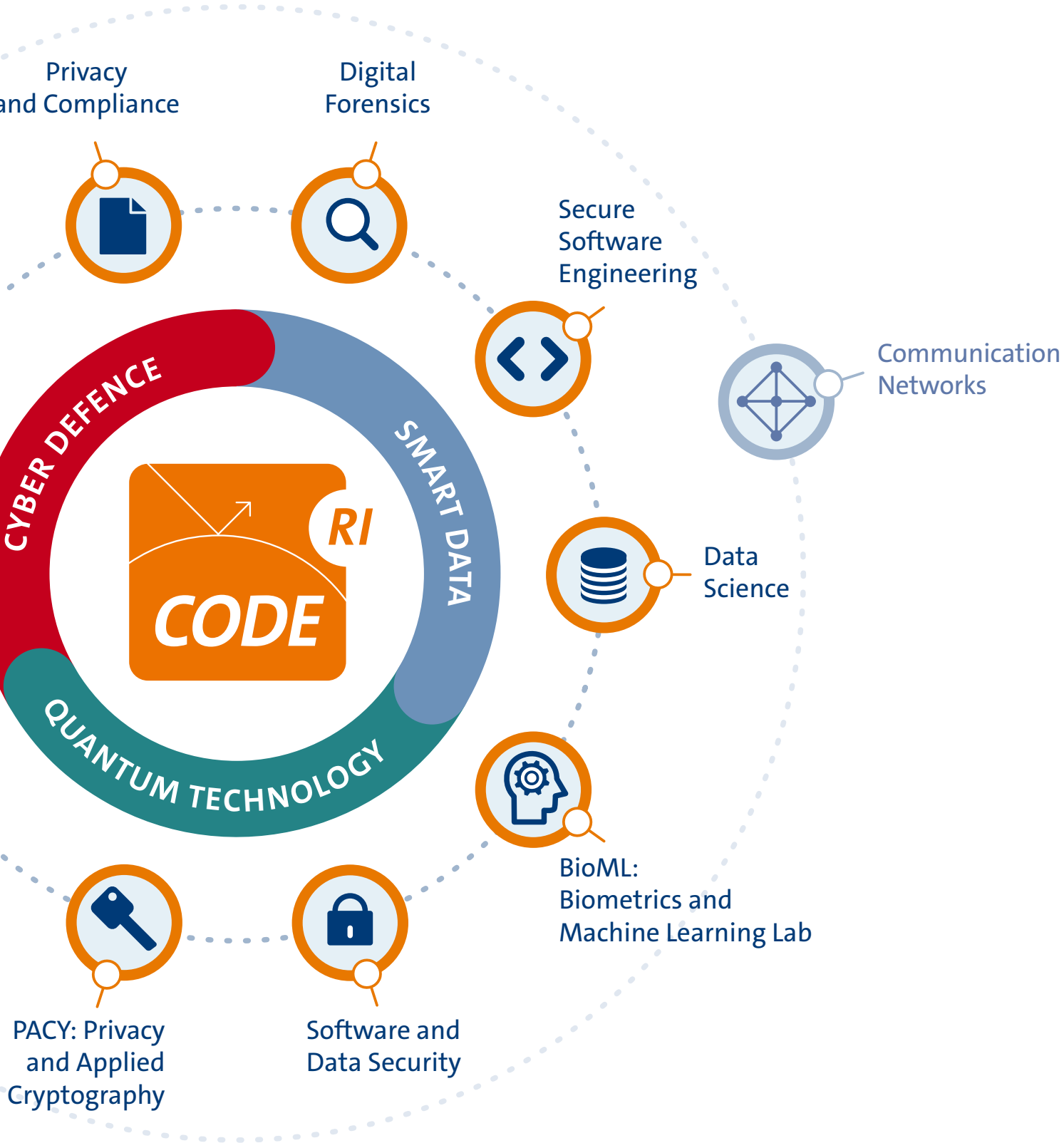
Research

Portraits and Projects

Research at RI CODE

In 2025, the various research groups at the Research Institute CODE carried out 48 third-party funded projects. A selection of these projects is described on the following pages. CODE conducts research in three overarching business areas: Cyber Defense, Smart Data, and Quantum Technology.

FIG.: TAUSENDBLAUWERK.DE


Privacy and Compliance
Digital Forensics
Secure Software Engineering
Communication Networks
Data Science
BioML: Biometrics and Machine Learning Lab
Software and Data Security
PACY: Privacy and Applied Cryptography
CYBER DEFENCE
SMART DATA
QUANTUM TECHNOLOGY
RI
CODE

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

Over the past years, the Munich Computer Systems Research Lab has focused its research efforts on Software-Defined Defense. As evidenced by invited talks and panel memberships at international conferences, as well as receiving a prestigious international award, we are considered as a leading research group providing coveted expertise.

BY UNITING BOTH professional recognition and successful organization of scientific events, the past year proved to be an enormous success for the Munich Computer Systems Research Laboratory (µCSRL).

From a project perspective, 2025 saw the conclusion of three major projects, APERITIF, DEMISEC, and DEPS. APERITIF provided funding for research activities in automated vulnerability identification. DEMISEC supported research in vulnerability identification in binaries. DEPS funded extensive research on protecting proprietary intellectual property through a unique mechanism that enables effective software to hardware binding.

The entire µCSRL research group attended the 41st Workshop of the GI special interest group on programming languages and computational principles in Bad Honnef. In addition, Prof. Brunthaler organized the 23rd "Kolloquium für Programmiersprachen und Grundlagen der Programmierung", in Feldkirchen-Westerham. This colloquium was founded by Friedrich Bauer from TU München, Klaus Indermark from RWTH Aachen, and Hans Langmaack from CAU Kiel. Prof. Langmaack was able to attend this 23rd colloquium and four generations of a single academic lineage were photographed (Prof. Langmaack, Prof. Knoop, Prof. Brunthaler, current µCSRL PhD students.).

The unquestionable highlight from a research perspective was the acceptance of our Tephra paper at the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE 2025), a top-ranked, highly selective and prestigious conference. Tephra also won the ACM SIGSOFT distinguished paper award at ASE, recognizing the value the scientific community places in µCSRL's research and the reported results.

Summing up, continued its Clausewitz-inspired journey "language-based security is the continuation of compiler construction by other means."

Prof. Brunthaler gave invited talks at the 11th AMSec workshop at the Vrije Universitäit Amsterdam, the Ministry of Defense, and the CyCon 2025, the international conference on cyber conflict in Tallinn, Estonia, where Prof. Brunthaler was also a panel member. He also served on the jury of the Dutch Cybersecurity Competition. In addition, µCSRL hosted a visiting researcher for the first half year of 2025: Giacomo Priamo from La Sapienza in Rome conducted research in automated program repair leveraging PL-semantics.

The µCSRL research group received funding from the German Ministry of Defense, the Austrian Research Promotion Agency (FFG), Hensoldt, and Oracle Labs.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

www.unibw.de/ucsrl-en

FIG.: ISTOCK / DE M10

Discovering the Limits of Fuzz-Testing Systems

Semantics-guided Synthesis to Evaluate Fuzzer Capabilities

TEPHRA is a principled methodology that uses semantics-guided synthesis to generate bug-free programs with diverse obstacles and statistically evaluate a fuzzer's ability to overcome them. We generated 21 obstacles and empirically evaluated the bypassing abilities of 31 contemporary fuzzers, consuming 37 CPU years. TEPHRA revealed limitations in current fuzzing heuristics and uncovered bugs in the fuzzers themselves.

Fuzz Testing

Fuzz testing (or fuzzing) was introduced in 1990 as a low-cost testing method that feeds a program random inputs and monitors for crashes. Since then, research in industry and academia has transformed fuzzing into a principled technique that complements established verification and validation methods to improve program correctness. Coverage-guided fuzzing now operates as a stochastic process that samples a program's state space, biased toward discovering new code or dataflow paths. This progress has enabled coverage-guided fuzzers to automatically find bugs in complex real-world systems such as web browsers, databases, operating systems, and security-critical libraries.

However, the general problem of program validation and bug finding is undecidable. As a result, fuzzers rely on heuristics. A fuzzer is therefore a set of ad hoc techniques that often work in practice but may fail in specific contexts. Unlike sound and complete methods such as abstract interpretation, bounded model checking, or interactive theorem proving, fuzz testing lacks a fundamental theory. We evaluate its effectiveness entirely through empirical data, including benchmark results and real-world fuzzing outcomes.

Empirical observations show that for every non-trivial program, a coverage-guided fuzzer eventually reaches a coverage plateau. At this point, it stops making progress even though further coverage is possible. The fuzzer fails to generate inputs that reach unexplored states and thus misses potential bugs. In other words, the fuzzer gets stuck.

Yet we lack a systematic understanding or approach for overcoming such obstacles.

A New Approach: TEPHRA

To tackle this problem, we created TEPHRA, a principled methodology for evaluating a fuzzer's ability to explore hard-to-reach program states. Unlike existing bug-finding benchmarks, TEPHRA takes a fundamentally different approach. It relies on pseudorandom semantics-guided program synthesis to generate obstacle snippets of varying complexity, and uses an analytical model to measure fuzzer bypassing ability with statistical guarantees. TEPHRA's bottom-up, grammar-driven synthesis enables the generation of diverse obstacles that probe the space of program semantics.

Additionally, our work contributed an empirical study, comprising over 37 CPU years of computing time, to investigate the limits of 31 different fuzzing systems, using different C and C++ obstacles.

TEPHRA was peer-reviewed and published at the International Conference on Automated Software Engineering (ASE) held in November 2025 in Seoul, South Korea, where it got recognized with a distinguished paper award.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

https://ucsrl.de/research/tephra

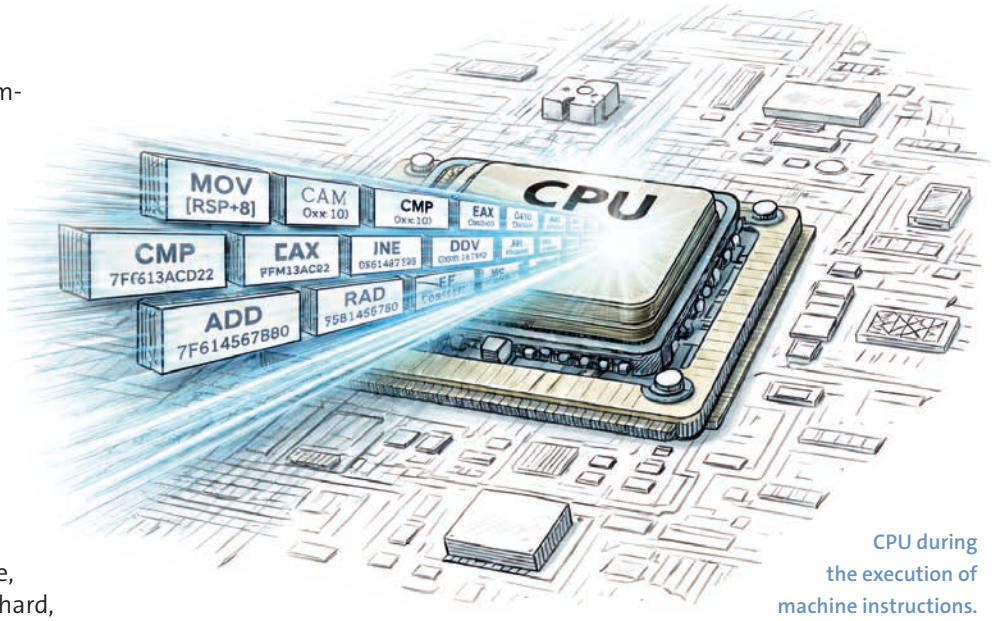
Empirical Investigation of Program Semantics

Data-driven Compiler Design Through Large-scale Semantic Analysis

In this project, we analyze a large corpus of system programs across languages and architectures to identify common semantic traits. These traits enable compilers to apply fast heuristics to frequent cases while reserving expensive methods for the rest.

Background

General-purpose programming languages are usually Turing-complete. For economic reasons, computing hardware (e.g., CPUs) is also designed to be as general-purpose as possible. As a result, programming-language processors (e.g., compilers and interpreters) must handle many computationally hard and sometimes undecidable problems. For example, register allocation is NP-hard, and constructing a complete and sound control-flow graph for an arbitrary program is undecidable. Thus, a sound compiler must use computationally expensive algorithms for hard problems and make conservative assumptions when facing undecidable ones.



CPU during the execution of machine instructions.

In practice, however, compilers employ fast heuristics for common cases and reserve sound but expensive solutions for fallback. This raises an important question for compiler designers: *What are the common cases?*

If a compiler knows the semantic properties that characterize 80–90% of its inputs, it can make data-driven decisions rather than relying solely on developer intuition. If, for example, most input programs exhibit structured control flow, a compiler can choose a simpler and faster control-flow graph construction algorithm.

Approach

With this ongoing project, we conduct a large-scale study of empirical traits in system programming language semantics. In particular, we compile a carefully selected corpus of C, C++, Go, Rust, and Ada programs to x86, ARM, RISC-V, PowerPC, and SPARC, and analyze multiple metrics at several abstraction levels of the translation process.

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

FIG.: S. BRUNTHALER (GENERATED WITH AI)

Prof. Dr. Michaela Geierhos

Data Science

The interdisciplinary team of the Professorship of Data Science combines expertise from the fields of computer science, business informatics and computational linguistics to address current and future-oriented research questions in the areas of semantic information processing and knowledge & data engineering.

Applied Research

Data science is an applied, interdisciplinary science. Its aim is to generate knowledge from data, for example in order to support decision-making processes. It uses methods and insights from fields such as statistics, computer science, and computational linguistics.

The Professorship of Data Science researches methods for extracting information from data and develops data-driven solutions by processing, preparing, analyzing, and inferring large amounts of data (Big Data). This includes, among other things, the development of algorithms for (semantic) text analysis, which find practical application in social media mining, for example, which in turn can be used to identify threats to protected objects. The type of data is very diverse: in addition to text, audio signals and images are also processed.

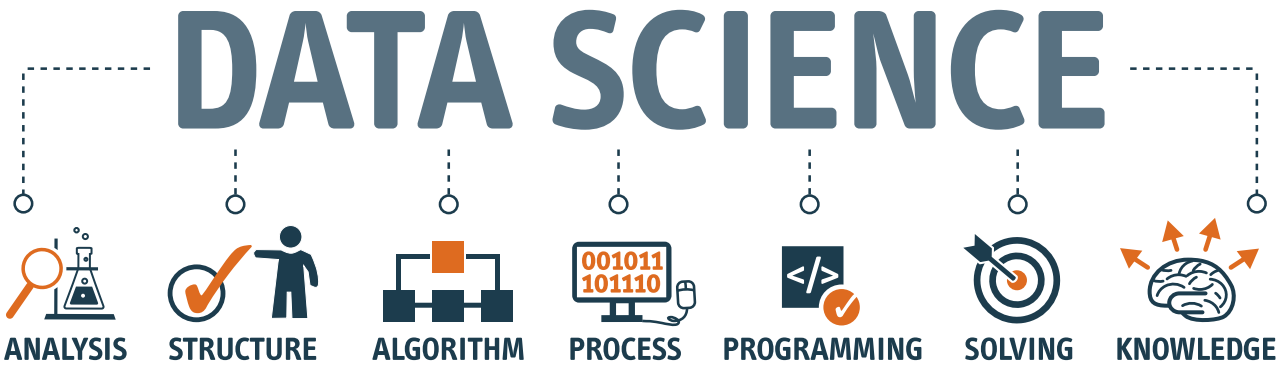
Practice-oriented Training

All Data Science courses are based on a teaching concept that combines theory and practice. Right from the start, students benefit from the opportunity to directly apply the theoretical knowledge acquired in the lectures in a variety of exercises and diverse practical projects. In this way, the Professorship of Data Science contributes to the excellent academic education of students at the University of the Bundeswehr Munich.

Data Science Use Cases: Practice-oriented Research

The Data Science team maintains numerous collaborations with partners from the military, business, and the public sector in order to link theory and practice in research as well. The areas of application currently range from the use of trustworthy AI in police applications to the reconstruction of audio data and the dynamic extraction of news narratives from various news articles for cyber threat analysis. One research goal is to identify and evaluate cooperation partners based on patent information. This year, the first prototype of the KiTIE tool was made available to various research institutions for testing purposes. The feedback was very positive, and previously unknown potential partners were also identified. In addition to quantitative evaluation, qualitative feedback was also obtained and both were integrated into the tool. With this improved version, the second test phase is now beginning. The VIKING (Trustworthy Artificial Intelligence for Police Applications) joint project investigated interdisciplinary methods for developing, evaluating, and securing trustworthy AI for police use. The focus here was on explainable AI language models for transparent text classification by security authorities. The background to this was the challenge of efficiently evaluating large amounts of text data in police work without accepting risks to individuals and society due to incorrect or biased model decisions. A key result was a system for the semantic modeling of police reports that structures complex content and makes it quickly usable. In addition, visualizations for bias assessment, debiasing procedures, and local explanations were implemented.

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



Range of tasks covered by the Professorship of Data Science.

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

SynData

Robust Detection and Analysis of Synthetic Media

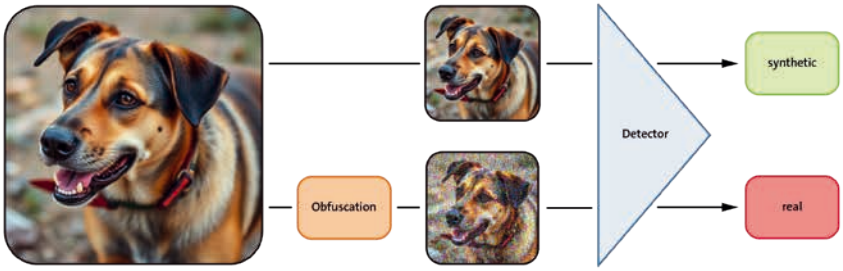
Modern AI-based programs allow users to generate deceptively realistic image data in just a few clicks. This has led to increasing misuse, such as for disinformation, fraud, or other harmful purposes. The SynData project addresses this issue. It aims to help better understand the underlying generation process while also making the detection of artificially generated image data more reliable.

Project Overview

The SynData project consists of two research teams with different areas of focus. One team investigates methods for detecting synthetically generated images, while the other focuses on obfuscation techniques designed to protect generated images from common detection methods. This parallel development creates valuable synergies: detectors can be continuously improved, while at the same time more effective obfuscation methods emerge, which in turn serve to test the robustness of the detectors. Over the past two years, both teams have developed and evaluated several solution approaches for synthetic image detection and obfuscation in line with their respective research priorities.

Development and Evaluation of Detection Methods

In the field of image analysis, pixel-based models are typically employed for image classification. These models learn characteristic artifacts in synthetic content and are therefore able to distinguish between real and generated image material. Based on this foundation, several new detection models have been developed that reflect the current state of research and, in some cases, demonstrate significantly improved detection performance.



A detector attempts to distinguish between real and synthetically generated images. Obfuscation techniques conceal features relevant to the detector by making slight adjustments to the pixel values of the generated image.

Development and Evaluation of Novel Obfuscation Methods in the Context of Synthetically Generated Images

The Data Science team initially conducted fundamental research on the topic of obfuscation. Specifically, a comprehensive study was carried out on the core topic of the "visibility of obfuscation artifacts" and its results were evaluated with respect to key visual criteria. The results form the basis for assessing novel obfuscation methods.

Building on these insights, a novel obfuscation technique was designed that hides the typical visual artifacts of such methods from human observers. In addition, a method was developed to ensure the effectiveness of obfuscation techniques even after image compression. This is particularly relevant since synthetic content is often distributed via web platforms that apply compression. This further underscores the importance of robust detection methods.

The obfuscation techniques developed in the project modify synthetic images in such a way that both protection against detectors is strengthened and visible artifacts are reduced. The models developed within the project are used to systematically evaluate the robustness of the deployed detection systems.

FIG.: RI CODE / A. SOARES DE SOUZA

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

ADRIAN

Authority-Dependent Risk Identification and Analysis in online Networks

ADRIAN makes hidden threats to web users visible: it constructs consistent digital twins from publicly available data in social networks. On this basis, quantitative indicators assess the risk of identity theft and spear-phishing on the web, thereby making privacy threats measurable.

Online Information as a Source of Risk

Information disclosed on the web, no matter how inconspicuous it may appear, can pose a security risk when combined with other data points. Social networks play a key role in this context, as they offer a wide range of content that can be analyzed and cross-referenced by third parties. The associated risks are real and multifaceted: they range from burglars who use visible vacation photos and absence notifications to plan break-ins to the takeover of digital identities that can lead to the misuse of accounts and personal information.

Digital Twins as a Tool for Threat Analysis

The challenge is that users of social networks can hardly recognize which attack vectors emerge from their digital footprint, which grows both knowingly and unknowingly. Individual pieces of information may seem harmless, but in combination they can form an accurate personal profile. This is where the project begins: the goal is to make relationships within data visible, assess risks and warn users so that they can take appropriate security measures.

As studies show, users maintain on average seven to eight profiles across social networks, resulting in numerous scattered fragments of information which, when aggregated, can form a comprehensive personal profile. ADRIAN addresses this issue with a framework that consolidates information from heterogeneous profiles into consistent digital twins using data-driven aggregation methods. On this basis a threat model was developed that combines machine learning techniques with information-theoretic concepts. This enables both the computation of identity theft risk and the assessment of vulnerability to spear phishing attacks. The resulting metrics indicate how attractive a potential target is and how easily an attack can be tailored.

Synthetic Content Introduces New Attack Vectors

Against the backdrop of increasingly powerful multimodal models, the analysis of synthetic content such as deepfakes or AI-generated social media profiles is gaining importance. Current work examines how synthetic digital twins can be generated. These are used to analyze attack vectors and to develop methods that distinguish real from synthetic digital twins. In this way ADRIAN expands its threat analysis framework to include the detection and evaluation of fake content.

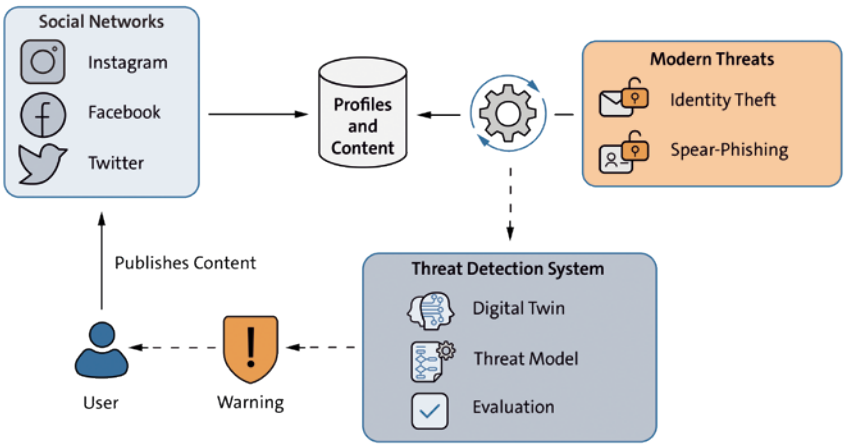


FIG.: HSBI / S. SCHULTENKÄMPER

Idea of the planned threat detection system.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

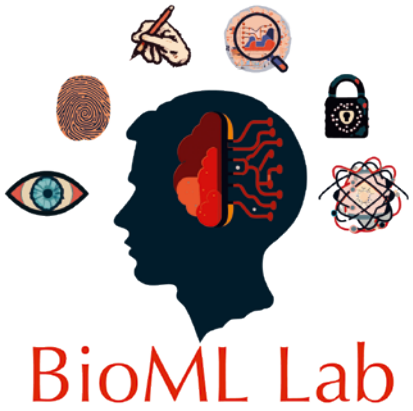
https://go.unibw.de/adrian-en

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.

Prof. Dr. Marta Gomez-Barrero

Biometrics and Machine Learning Lab

The BioML Lab, led by Prof. Dr. Marta Gomez-Barrero, holder of the Professorship of Machine Learning, researches methods to develop reliable, secure, fair, and privacy-friendly biometric recognition systems. The focus of the group is on highly innovative and applied IT-security interdisciplinary research, building upon machine and deep learning architectures as well as cryptographic methods.



BioML: Biometrics and Machine Learning research group.

THE Biometrics and Machine Learning (BioML) lab was established in October 2023 and is part of the Research Institute CODE and the Department of Computer Science. Led by Prof. Dr. Marta Gomez-Barrero, holder of the Professorship of Machine Learning, BioML researches methods to develop reliable, secure, fair, and privacy-friendly biometric recognition systems. The focus of the group is on highly innovative and applied IT-security interdisciplinary research, building upon machine and deep learning architectures as well as cryptographic methods.

BioML co-organizes and participates in international academic conferences such as the IEEE Int. Joint Conference on Biometrics (IJCB) and the IEEE Int. BIOSIG Conference and contributes both to the European Association for Biometrics (EAB) and the international standardisation in ISO/IEC JTC1 SC37.

Research Foci at the BioML Lab

Biometric recognition refers to the automated recognition of individuals based on their behavioral and biological characteristics. Examples of such characteristics within the scope of the group include face, iris, fingerprint, finger vein, electrocardiograms or handwritten signatures, as well as combinations of those in multi-biometric schemes. Besides trying to increase the recognition accuracy and computational efficiency of the systems, the lab focuses on other relevant aspects of this research area. Preserving the privacy of the subjects is at the core of the research, for which the lab develops biometric template protection schemes in compliance with the General Data Protection Regulation (GDPR) and relevant ISO standards, following the Privacy-by-Design principle. Furthermore, the detection of several forms of attacks on biometric systems (e.g., Presentation Attacks or Morphing Attacks) is key to increasing the security and reliability of the systems. Last but not least, the team aims at explainability and transparency of the algorithms to allow further acceptance and deployment of biometric recognition.

Activities

In 2025 the main research lines at the BioML Lab were continued: biometric template protection for privacy-friendly biometric systems, presentation attack detection with both autoencoders or large language vision models, and the analysis of biometric quality for synthetic images produced with generative AI architectures. Osman Demir presented his work on deep hashes for iris template protection in Darmstadt during the BIOSIG 2025 conference.

On an internatonal level, the BioML Lab has reinforced its collaborations through different activities. Prof. Gomez-Barrero has finalized the Springer “Handbook on Biometric Template Protection”, together with Vedrana Krivokuca and Sébastien Marcel from Idiap (Switzerland) and Arun Ross from Michigan State University (USA), which will be published in January 2026. In April, BioML hosted at the UniBw M the 13th edition of the IEEE Int. Workshop on Biometrics and Forensics (https://www.unibw.de/iwbf2025), which attracted participants from within and outside Europe and two excellent keynotes from Meike Ramon (University of Lausanne) and Xiaoming Liu (Michigan State University, MSU).

Marta Gomez-Barrero continued leading the review process of the ISO/IEC standard 30136 on “Performance testing of biometric template protection schemes”, which has reached a DIS stage after the last ISO SC 37 meeting in Singapore in July 2025. Through the European Association for Biometrics (EAB), she co-organized the Martigny Biometrics Workshop with the US Center for Identification Technology Research (CITeR) and the Idiap Research Institute. In addition, she co-organized once again the Darmstadt Biometrics Week together with the Fraunhofer IGD.

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

FIG.: ADOBE STOCK / DILOK; RI CODE / MARTA GOMEZ-BARRERO

MLLMs meet Biometrics

Can Multimedia Large Language Models Help Detect Attacks on Biometric Systems?

We are now used to utilize face recognition systems on a daily basis, for instance to unlock our smartphone or to cross the border at the airport. It is indeed a convenient and accurate recognition method. But as any other IT-system, these methods are vulnerable to attacks – and our goal is to detect those, in order to provide a more robust and reliable experience.

Biometric Presentation Attacks

Among the different attack points of biometric recognition systems, the sensor or capture device is the most vulnerable one: the attacker needs no deep understanding of how biometric recognition is carried out. They just need to fabricate a fake biometric characteristic, such as thin fingerprint overlay made of latex, or a 3D silicone face mask, to fool the system. It does not matter whether they want to impersonate another person or just avoid being recognition – such attacks are known as presentation attacks. Since these pose severe security threats for our systems, the biometrics community, and the BioML Lab, has been working for years on how to automatically detect presentation attacks with additional modules known as Presentation Attack Detection (PAD) mechanisms.

Face masks can be used to launch a presentation attack on biometric systems.

FIG.: ADOBE STOCK / DREAMSTOCK (AI GENERATED)

Multimedia Large Language Models (MLLMs) for PAD

In the past, either traditional machine learning algorithms such as Support Vector Machines (SVMs) based on texture features, or more recently, deep learning architectures such as Convolutional Neural Networks (CNNs), have been used as PAD modules. However, as technology evolves, more complex attacks appear. But also more reliable tools to detect them.

such as Large Language Models (LLMs) have been primarily designed for text-based applications and have already been successfully employed for a large number of very diverse tasks. Multimodal LLMs (MLLMs) are their natural evolution and can process and generate text, images, and audio, delivering significant capacity to improve biometric systems; however, this potential has not been fully investigated so far. We are thus investigating how large vision-language models (LVLMs) can be leveraged to detect presentation attacks in biometric systems, with an emphasis on their baseline zero-shot and few-shot performance. To that end, we have analyzed several models, including Gemma, Qwen and Pixtral, on four different and standard facial presentation attacks databases in our experiments, and tested several combinations of system and user prompts.

The results have been very promising so far: we achieve error rates under 5% in the first benchmark. However, other scenarios lead to higher error rates up to 23%, and some attacks are more challenging to detect than others. This motivates us to pursue this line of work further with end-to-end fine-tuning of the models further parameter optimization.

Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml-en

Biometrics and Privacy

Can We Generate Different Templates from a Single Iris?

It is now well-known that biometric systems offer a number of advantages with respect to authentication methods based on passwords or tokens: for instance, you cannot forget your face at home and you cannot pass it on to another person (i.e., there is a stronger link between subject and authentication item, and you cannot repudiate an authentication attempt you did in the past). However, there are also some challenges: how can we revoke a compromised iris template and generate a new one? How many times can we do this?

What is Biometric Template Protection?

Biometric data is classified as sensitive personal data in the European General Data Protection Regulation (GDPR). In order to be able to use biometric systems, the data must therefore be protected throughout: during storage, transmission, and any type of processing. The ISO/IEC 24745 standard defines the properties that biometric template protection (BTP) schemes must fulfill, and the ISO/IEC 30136 standard contains guidelines for testing these schemes with regard to privacy protection.

Renewability and Unlinkability

Two of the aforementioned properties for protected biometric templates are renewability and unlinkability. The former refers to the process of generating a new template from the same biometric instance (e.g., your right iris) in case the existing one has been compromised. In essence, the same process of choosing a new password after a known leak. And, of course, the old and the new template cannot match.

Unlinkability somehow refers to a very similar property: one of the main advantages of biometrics is that you can re-use your right iris to enroll into different systems, without compromising their security, in contrast to the requirement of having different passwords for different systems. In order for this to work, however, we need to generate templates which do not match each other, but stem from your same right iris. One can view there two properties as the same attribute of protected biometric templates either in the time (renewability) or in the space dimensions (unlinkability). Thus, we can use the same metrics to evaluate both properties.

Using different app parameters, we can generate different unlinkable templates from a single iris.

Achieving Unlinkability

We still haven't addressed the main question; how can we achieve unlinkability? Most biometric template protection schemes incorporate some kind of parameter set or key to do this: by changing the key, we can generate a new, non-matching or unlinkable template. Again, similar as to what we would do if a cryptographic secret key would be compromised: we would need to generate a new key. And likewise, not all keys or passwords are equally good: if we chose two passwords which only differ in one character, the security of the system will probably decrease.

We are now investigating how these issues affect biometric template protection schemes based in Bloom Filters. These systems are general enough to be applied to different biometric characteristics (e.g., face, iris, fingerprint or combinations thereof), and have shown a strong unlinkability and a remarkable recognition performance with virtually no loss with respect to unprotected systems. To that end, we are simulating larger numbers of protected databases, each using a different permutation key (i.e., the key used by these systems to provide renewability and unlinkability), and measuring the unlinkability across all databases with the metrics provided within the ISO/IEC 30136 standard. The first preliminary experiments show constant unlinkability values for at least 200 different keys.

Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml-en

FIG.: ADOBE STOCK / TANYA (AI GENERATED)

Prof. Dr. Wolfgang Hommel

Software and Data Security

Wolfgang Hommel's team researches technical and organizational security measures for complex IT infrastructures and communication networks with an increased need for protection – from conception to practical development – under the guiding principle "Development and Operation of Secure Networked Applications".

THE PROFESSORSHIP OF Software and Data Security pursues the goal of developing solutions for real-world-security challenges while considering operational constraints, which are typically encountered in the management of complex IT infrastructures.

Research activities and projects with third parties usually begin with a comprehensive empirical analysis, in which, for example, relevant components from the designated application area are cloned into virtual environments or, at least, their core characteristics are modeled and simulated to facilitate a detailed vulnerability and risk assessment. This approach allows, among other things, the explorative application of offensive test procedures, enabling both qualitative and quantitative analyses of vulnerabilities within complex, multi-stage attack scenarios. The insights gained form the basis for systematically deriving security requirements that guide subsequent design activities and the practical evaluation of the resulting solutions.

The design and advancement of IT security measures follow a security engineering approach: (New) measures are designed, modeled, and simulated on a technical level and, additionally, integrated as seamlessly as possible into the design, implementation, and operational processes of the intended application domains, also from an organizational perspective. An essential objective is the hands-on implementation with subsequent evaluation – at least in laboratory settings, preferablyin pilot environments, and ideally within scientifically supervised real-world projects. In addition, the team considers the human factor in information security as well as economic and legal constraints to ensure holistic and sustainable security solutions.

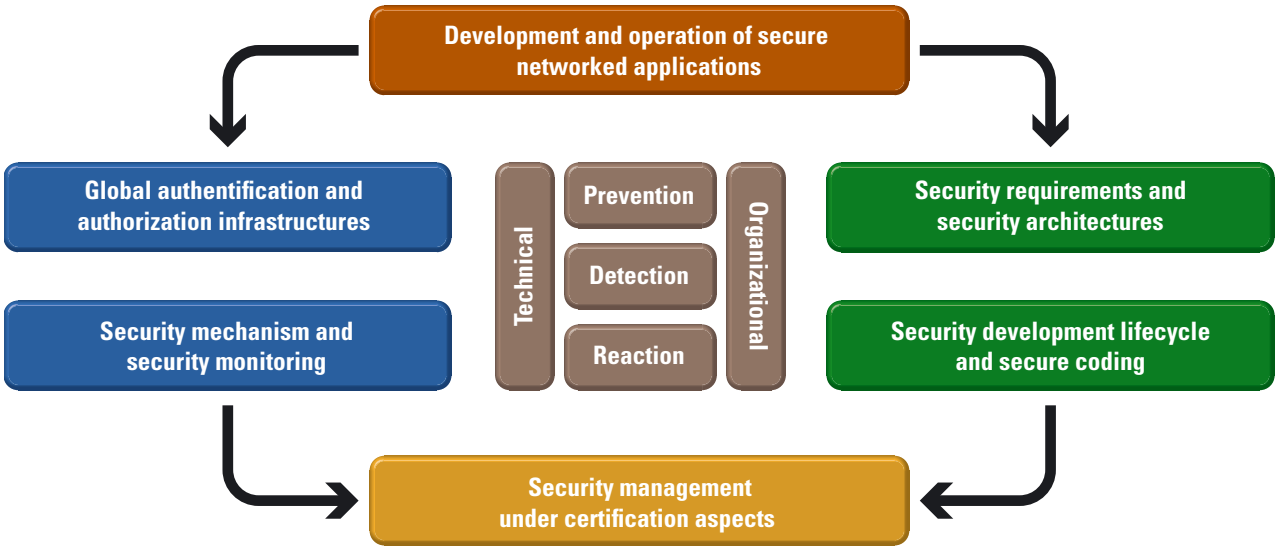
Current research projects and funded initiatives in 2025 included research concerning quantum communication infrastructures based on quantum key distribution, security management for future 6G networks, and the secure operation of modern energy supply networks. Practical transfer with partners from industry and the public sector also plays an important role: for example, the second generation of the prototypical, black-out-proof crisis communication system MERLIN was put into operation as part of dtec.bw; the application of LoRa radio technology, which is used for civil disaster control here, with regular crisis management exercises provides empirical experiences that can also be transferred to use in the German Armed Forces.

Prof. Dr. Wolfgang Hommel

wolfgang.hommel@unibw.de

+49 89 6004 7355

www.unibw.de/software-security



Main research topics of the Professorship of Software and Data Security.

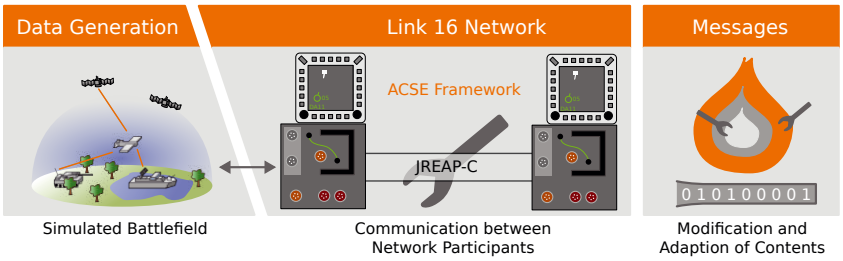
FIG.: ISTOCK / VERTIGO3D; TAUSENDBLAUWERK, QUELLE: RI CODE / WOLFGANG HOMMEL

Airborne Cybersecurity Enhancement Long-Term Evolution

Tactical Data Links — Examined Bit by Bit

Tactical data links are communications protocols and techniques specifically designed to exchange tactical data between units. This data can include troop movements, reconnaissance findings, and orders. The aim of this project was to intervene in the flow of information at the bit level in order to model interference. The goal is to use these results to improve the resilience of such data links.

MILITARY UNITS use tactical data links (TDLs) to share information about their status and surroundings with other units. This lets units build a picture of the environment beyond their own sensor coverage, and it enables commanders to make faster, better-informed decisions about how to employ their forces based on the emerging operational picture. A critical factor here is the correct transmission and processing of the data.



Sketch of the demonstration setup. Information from a synthetic battlefield is being exchanged between two Link 16 emulators. There it is intercepted by the ACSE Framework which analyzes and modifies the traffic.

ACSE – The Concept

Every digital communications system uses dedicated message formats to exchange information between communicating peers. Multiple protocol layers often work together to ensure end-to-end delivery. Especially with complex protocols, gaps in a specification or its implementation can be exploited by adversaries. Extensive testing is therefore essential. In the predecessor project — ACSE — we developed testing methodologies and prototyped a corresponding framework. Using it, message formats and the logic of communication endpoints can be flexibly emulated and modified at any desired level of granularity. This allows real protocol implementations to be tested in parallel to their normal development cycle, against an independent implementation. To reduce engineering effort, development focused in particular on enabling data import from existing machine-readable specifications.

Implementation for Link 16

In ACSE LTE, the existing methodology and framework were extended to support TDLs. Link 16 (STANAG 5516) over JREAP-C (STANAG 5518) was selected as the demonstration target, since this combination of standards is widely used within NATO. With these extensions, the framework could be used to modify transmitted data down to the bit level and make subtle changes to logical content. Because of dependencies within and across protocols, even tiny changes can invalidate a message — for example, when checksums no longer compute correctly. The framework encodes these dependencies and can, if desired, automatically apply adjustments to restore a message's syntactic correctness.

Tests were conducted at Airbus DS using both synthetic real-time data and recorded data in an Airbus Integration Prototyping Lab. The seamless integration with existing test tools (e.g., Link 16 simulators) was also validated.

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

Funded by: Airbus Defence und Space

FIG.: RI CODE / A. FRANK

ROLORAN

Resilient Operation of LoRa Networks

The dtec.bw project ROLORAN investigates the performance of the energy-efficient LoRa ("Long Range") radio technology with partners from the military, government, research, and industry. Beyond range, interference resistance, localization, and mesh networking, the project focuses on attack detection, secure operation, and developing hardware and software for complex LoRa networks and field testing.

SECURE AND reliable communication via radio links is of central importance, particularly in the (Military) Internet of Things. In scenarios connecting many sensors and actuators (with or without centralized infrastructure) resistance to interference, scalability, low weight, battery operation, and agile network topologies (e.g., through mesh and swarm capability), as well as simple software adaptability, are often essential. In contrast, lower data rates are generally bearable.

The chirp spread spectrum–based modulation LoRa represents an adequate tool for various applications due to its long range, low acquisition and operating costs, and energy efficiency. Further, LoRa is complemented by the standardized LPWAN protocol LoRaWAN, which enables data aggregation and analysis in a backend via gateways, using both commercial and open-source software stacks.

Pushing Performance Boundaries

Since 2021, the dtec.bw project ROLORAN has been systematically testing and developing its own hardware and software components for LoRa and LoRaWAN infrastructures. In addition to investigating transmission ranges indoors and outdoors under varying circumstances, the project examines reconnaissance, localization, jamming, and frequency agility of LoRa devices. Furthermore,

Demonstrator for the localization of LoRa transmitters with route planning to its location (top left); Excerpt of data analysis for flash flood detection (top right); ROLORAN prototype „LoRa Field Testing Device (LoRa FTD)" (bottom left); Energy-autonomous MERLIN base in Neuhaus (bottom right).

proprietary LoRa-based communication protocols (e.g., for mesh topologies) and prototypes cost-effective multi-channel LoRa radios are developed. Several generations of these in-house prototypes demonstrate mobile and deployable use, including in UxV contexts, and the applicability of the technology for data exfiltration, area and perimeter surveillance, as well as Blue Force Tracking.

Putting Research into Practice

In line with dtec.bw's goal of transferring research into practice, ROLORAN has already realized LoRa installations with the Austrian Armed Forces in the field of facility management and with the Bavarian district of Bad Kissingen for establishing a sensor network for flash flood early warning. In 2025, the second generation of a blackout-resistant crisis communication infrastructure based on the ROLORAN Disaster Communication Protocol (RDCP) was commissioned in the municipality of Neuhaus in Carinthia and released as open source. This fall, a prototype for transmitting vital data in medical applications was implemented to demonstrate the technology's usability in particularly sensitive environments. Currently, work is underway on dedicated security sensors for LoRa-based networks and on methodologies for IT-secure, seamless integration of LoRa components into existing systems, platforms, and infrastructures.

Mario Silaci

mario.silaci@unibw.de

+49 89 6004 2846

https://go.unibw.de/roloran

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – Next Generation EU.

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

Prof. Dr.-Ing. Mark Manulis

Privacy and Applied Cryptography Lab

The PACY Lab, led by Prof. Dr.-Ing. Mark Manulis, holder of the Professorship of Privacy, researches technologies for improving privacy based on modern cryptographic methods. The focus is on the design, analysis and development of cryptographic methods for the protection of users, data and messages, as well as their practical use in Web, Cloud, IoT and Blockchain applications.

Research Focus at the PACY Lab

The PACY Lab was established in March 2022 and is part of the RI CODE. Its research staff has in-depth knowledge of cryptography, computer science and mathematics, which they successfully use for foundational and applied research.

The lab explores methods and technologies in the area of Privacy Enhancing Cryptography (PEC), which includes all sorts of cryptographic schemes with extended requirements on confidentiality and privacy.

The PACY Lab focuses on the design and practical use of various PEC methods, including advanced encryption and signature schemes and relevant cryptographic protocols. The lab works on modelling and analysis of their functional properties and protection goals. Dependencies between methods and properties are explored to improve their general understanding and identify new design strategies. The PACY Lab develops new PEC procedures and uses them to develop cryptographic protocols for authentication and access control, processing of data and transactions, and secure messaging.

In the design and implementation of new PEC approaches, the PACY Lab deploys mathematical techniques that are commonly used in cryptography such as elliptic curves and bilinear maps, and now more increasingly techniques from lattice-based cryptography in order to realize the desired security against future quantum computers. Other PEC techniques used at PACY Lab include secret sharing and zero-knowledge proofs.

PEC for Data: Access Control and Data Processing

Traditional encryption methods can provide data confidentiality but cannot be used directly for processing encrypted data. Modern PEC methods allow a variety of operations on encrypted data without having to decrypt it during processing. The PACY Lab is working on functional encryption schemes offering better flexibility in access control and data exchange as well as enabling direct processing of encrypted data in distributed multi-user applications. Ongoing research includes approaches for fully homomorphic encryption and attribute-based encryption as well as cryptographic protocols supporting operations (e.g. search queries) on encrypted data, along with their use in distributed applications.

PEC for Users: Authentication and Message Exchange

Digital signatures form the backbone of modern PKI. With them, users can authenticate themselves or establish end-to-end secure communication channels. The verification of PKI-based signatures reveals a lot of sensitive information, such as identities, public keys and all attributes. The PACY Lab is researching advanced signature techniques to combine authentication with anonymity or untraceability. Ongoing research includes attribute-based signature schemes and related concepts behind anonymous credentials schemes. In addition, the PACY Lab is researching security protocols for secure and private messaging and for distributed and delegable authentication, for example in connection with the new FIDO2 standard for web authentication.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy-en

FIG.: ADOBE STOCK / A. YALANSKYI; RI CODE

PiQASO: Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures

Secure Transitioning to Post-Quantum Cryptography

The PiQASO project aims to deliver a fully optimized and operational PQC-as-a-Service framework, offering a suite of quantum-safe cryptographic protocols – covering key encapsulation, digital signatures, authenticated key exchange, authorization, identity management, and long-term data protection. This framework aims to provide a complete, quantum-resistant PKI equivalent that is both secure against future quantum threats and practical for seamless integration into existing transmission systems and infrastructures, without requiring additional client-side hardware, enabling quantum-safe encryption and decryption for legacy systems.

An Overview of the PiQASO Project

The PiQASO project is a multi-national consortium of two academic institutions and 23 industrial partners from 12 EU countries. The project, which started in January 2025 and will be running for three years, is strategically designed to achieve critical outcomes that will pave the way for a secure and resilient digital future in the face of quantum computing advancements. The core technical innovation is PiQASO's quantum-safe and flexible PQC-as-a-Service framework. This is a cloud-based security solution that delivers PQC operations as on-demand services. It integrates optimized implementations of NIST-approved algorithms (incl. Kyber, Dilithium, etc.) to provide encryption, authentication, digital signatures, and key management across the edge-to-cloud continuum. Key features include crypto-agility, API-based integration for legacy and modern systems, modular authentication supporting classical and PQ certificates, secure key provisioning through a key management system, and certifiable end-to-end data protection. The framework will be validated through pilot use cases across diverse industries, incl. automotive, automation, finance, energy, healthcare, aerospace, online media, unmanned aerial vehicles, and transportation, demonstrating quantum-safe encryption, authentication, and data protection in real-world industrial environments.

PACY Lab's Role in the PiQASO Project

As a core technical partner, PACY Lab is involved in the specification and implementation of several cryptographic algorithms within the PiQASO's PQC-as-a-Service framework. Specifically, we are working on quantum-safe techniques for encrypted data storage, transmission, and sharing using updatable public key encryption (UPKE) to ensure long-term confidentiality and privacy. We are exploring novel, standards-compliant quantum-safe UPKE designs, employing Asynchronous Remote Key Generation (ARKG) techniques, which we have been developing since 2020, for scalable, future-proof cryptographic protection. In addition, we contribute to training and capacity building, helping develop educational materials for the PiQASO PQC Academy, which aims to raise awareness and skills in post-quantum cryptography across European industries.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

https://www.piqasoproject.eu

Founded by: EU through European Cybersecurity Competence Centre, Digital Europe (No. 101190366)

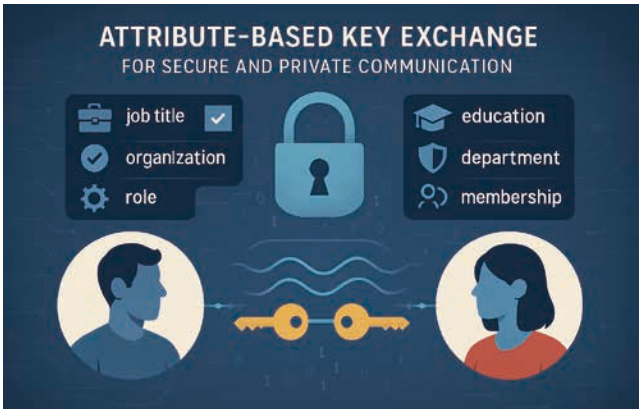
Attribute-Based Key Exchange with Optimal Efficiency

Enabling Fast and Secure Establishment of Cryptographic Session Keys Based on User Attributes

Attribute-Based Key Exchange (ABKE) is a cryptographic technique that allows users to establish a shared session key when their attributes satisfy a predefined policy. This mechanism extends traditional key exchange protocols by incorporating fine-grained access control directly into the key establishment process. ABKE has broad applicability in secure communication systems, i.e., ranging from client-server authentication to decentralized, role-based networking, where users can negotiate encrypted channels without revealing their identities.

Challenges in Attribute-Based Key Exchange

Designing efficient and secure ABKE protocols remains a challenging problem. Existing constructions often suffer from high computational and communication overheads, primarily due to the complexity of the underlying attribute-based encryption (ABE) mechanisms. Many known schemes rely on selectively secure ABE and inefficient pairings, which limit scalability and practical deployment. Another limitation is weak authentication – some schemes are susceptible to impersonation attacks or lack full perfect forward secrecy (PFS). The main challenge lies in building ABKE protocols that simultaneously achieve adaptive security, impersonation resistance, PFS, and optimal efficiency in both computation and communication.



Secure key exchange between two parties based on certified attributes or roles without revealing identity.

Building Fast and Expressive ABS Schemes

The PACY Lab, in collaboration with international partners, addressed these challenges by introducing a new generic and efficient construction of Attribute-Based Key Exchange (ABKE) that integrates fast attribute-based encryption (ABE) with two-pass authenticated key exchange (AKE) protocols. The approach builds upon recent advances in fast ABE, particularly the FABEO and FABESA schemes (developed in 2024 with our involvement), and efficient AKE protocols such as TOPAS and HMQV, combining their strengths to achieve adaptive security, PFS, and impersonation resistance. The proposed construction ensures optimal efficiency, allowing users to establish a shared session key with a constant number of pairing operations and minimal communication overhead. The protocol encrypts Diffie-Hellman ephemeral public keys using a fast ABE layer, enabling authorized users to decrypt and derive session keys securely. The scheme eliminates large group elements and avoids explicit digital signatures, reducing message sizes. A practical instantiation combining FABEO KP-ABE with PKI-based TOPAS demonstrated superior performance over existing ABKE schemes. Experimental evaluation showed that for a policy with 100 attributes, users can establish a session key in 0.15 seconds, including ciphertext generation, decryption, and shared key computation. This work, presented at CANS 2025, represents the first construction to achieve both enhanced security and optimal efficiency for ABKE.

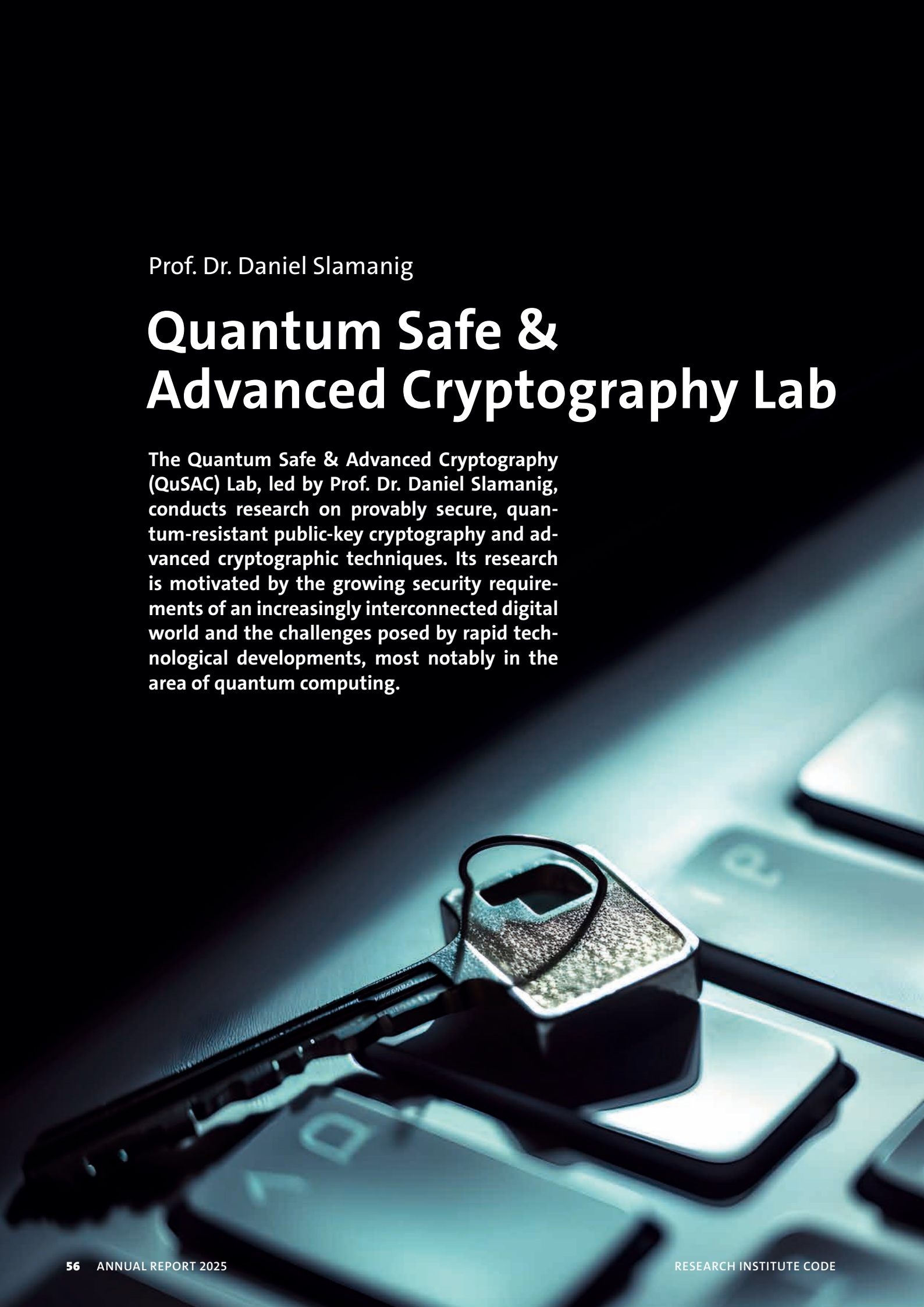
Prof. Dr.-Ing. Mark Manulis
+49 89 6004 7365
mark.manulis@unibw.de

FIG.: GENERATED BY DALL-E 3

Prof. Dr. Daniel Slamanig

Quantum Safe & Advanced Cryptography Lab

The Quantum Safe & Advanced Cryptography (QuSAC) Lab, led by Prof. Dr. Daniel Slamanig, conducts research on provably secure, quantum-resistant public-key cryptography and advanced cryptographic techniques. Its research is motivated by the growing security requirements of an increasingly interconnected digital world and the challenges posed by rapid technological developments, most notably in the area of quantum computing.



THE QUSAC LAB investigates both the theoretical foundations and practical applications of cryptography. Its research focuses on quantum-resistant public-key cryptography and advanced cryptographic primitives. The team develops modular constructions based on generic building blocks as well as schemes relying on concrete mathematical hardness assumptions. Provable security is a central methodological principle throughout QuSAC's work.

Relevance of Cryptography

Cryptography is a cornerstone of modern cybersecurity. It protects communication systems, digital identities and sensitive data across a wide range of applications. As contemporary digital infrastructures grow more complex, demands on the security, efficiency and functionality of cryptographic mechanisms continue to increase.

Stronger Security Properties – Quantum Computers and More

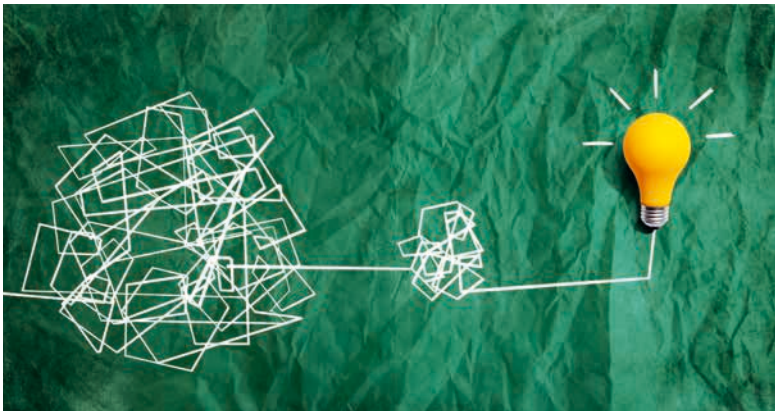
Progress in quantum computing threatens many of today's widely deployed public-key systems. Quantum-resistant (post-quantum) cryptography is therefore essential for future-proof security. We explore suitable mathematical problem classes, among them isogeny-based approaches, and develop cryptographic primitives built upon them.

Prof. Slamanig contributed, for example, to the development of the post-quantum signature scheme Picnic, which advanced to the third and final round of the NIST standardization process.

At the same time, basic primitives and their security guarantees are often insufficient for modern applications. We therefore work on advanced cryptogrpahic concepts with strong security properties as well as on the theoretical underpinnings of privacy-preserving cryptography.

More Functionality and Stronger Security

Modern applications increasingly require advanced functionality that goes beyond traditional cryptographic tools. A key part of QuSAC's research concerns non-interactive zero-knowledge proofs and their succinct variants (SNARKs), which are now widely used in practical systems. They provide strong security guarantees without compromising efficiency or scalability.



The challenge in cryptography is to solve problems that often seem paradoxical.

Contributions to the Academic Community

In 2025 Prof. Slamanig was invited to serve on the program committees of various top-tier conferences: 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). Moreover, he was invited to serve on the editorial board of the IACR Communications in Cryptology (CiC) and Proceedings on Privacy Enhancing Technologies (PoPETs) journal.

Development of the Research Group

Founded in November 2023, the QuSAC Lab currently hosts three doctoral researchers and one postdoctoral fellow. The group maintains a strong national and international research network, engages in numerous collaborations and regularly welcomes visiting scholars from abroad.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

www.unibw.de/crypto-en

FIG.: ADOBE STOCK / ANNIKA; ADOBE STOCK / TIERNEY

Post-Quantum Blind Signatures

New Protocols from Cryptographic Group Actions

Blind signatures are digital signatures where the signer issues a signature on a message without learning its content. They are a fundamental building block for applications that require privacy and control over the number of operations, such as e-cash and e-voting. For example, imagine a citizen who must have their electronic vote validated by the state without revealing their choice, while still ensuring they can vote only once; a blind signature provides exactly this balance between anonymity and one-time validity.

RECENT WORK has proposed post-quantum blind signatures mostly from lattice-based assumptions. However, to enforce diversity of security assumptions and to improve efficiency/robustness, we need alternative approaches that do not rely on lattices and avoid heavy zero-knowledge proofs, while preserving all security requirements ("blindness" and "one-more unforgeability") even when concurrent signing sessions are allowed.

Cryptographic Group Actions

Group actions generalize the discrete logarithm problem to settings where efficient quantum attacks are not known. Namely, given a set element x and the action, denoted by $g \star x$, of a (secret) group element g over x, the Group Action Inversion Problem (GAIP) consists in finding g. Group actions can be instantiated with isogenies (e.g., CSIDH, CSI-FiSh, and, more recently, PEGASIS), but also – in a noncommutative setting – with linear-codes (e.g., LESS).

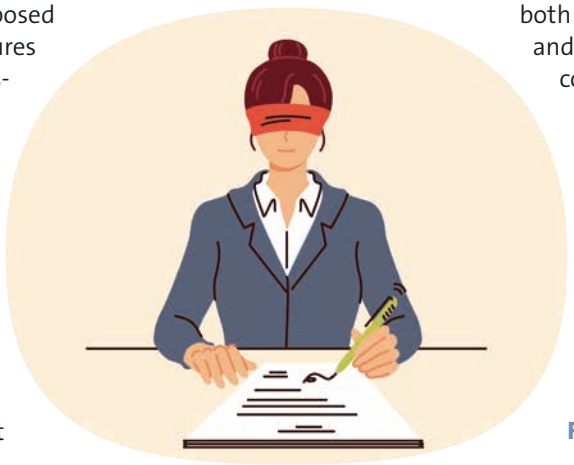


Illustration of blind signatures: A signer endorses a message she cannot read.

Our Contribution: Tanuki

In "Tanuki: New Frameworks for (Concurrently Secure) Blind Signatures from Post-Quantum Group Actions" (published in ASIACRYPT 2025), we introduce new three-move blind-signature protocols based on group actions. The core idea is to use random permutations to blind the signer's commitments, which are obtained from a fixed-weight hash of the challenges, i.e., a hash whose output always has the same number of 0s and 1s. The technique extends to the multi-key case and prevents known concurrent attacks. The frameworks admit instantiations both with isogenies (CSIDH/CSI-FiSh) and with codes (LESS), and reach compact signatures (e.g., ~4.5 KB with CSIDH and ~64.7 KB with LESS for 128-bit parameters in the concurrently secure variant). A crucial advantage is that our protocols do not require the action to be commutative and therefore cover a broad range of post-quantum assumptions.

Future Directions

In collaboration with the Norwegian University of Science and Technology (NTNU) and the CISPA Helmholtz Center for Information Security, we are also exploring new constructions of lattice-based blind signature schemes. The goal is to produce signatures whose structure and verification interface match those of a "conventional" signature scheme.

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

FIG.: SHUTTERSTOCK / APRINT

SPRINT: New Signatures and Proof System

New Isogeny Proofs of Knowledge and Signatures

As quantum computers become more powerful, many of today's cryptographic systems could be broken. Researchers are racing to develop post-quantum cryptography; systems that remain secure even against quantum attacks. One promising direction involves isogenies, special mathematical maps between elliptic curves. Isogeny-based signature schemes like SQIsign and PRISM are attractive because they produce very small keys and signatures, making them good candidates for future post-quantum security.

HOWEVER, THESE schemes also come with some drawbacks. Many of them rely on unusual or very complex security assumptions, which makes it harder for the community to fully trust them. Some require special mathematical setups or rely on curves with known internal structure, limiting how easily they can be used in different contexts. Others need complicated protocols to guarantee security, which can slow them down or make them harder to implement correctly. Because of these issues, researchers are still looking for isogeny-based signature schemes that are both simple to trust and practical to use.

The SPRINT Signature Family

Recent research by the QuSAC group aims to address these issues. They have developed a new family of very efficient digital signature schemes that build on existing post-quantum *polynomial commitment schemes* — a class of cryptographic tools that are used as building blocks to verify large computations quickly and securely. By combining these commitments with new techniques for proving knowledge of isogenies, the team created signature schemes that are not only fast to generate and verify but also rest on well-established mathematical assumptions.

SPRINT provides very efficient proofs of knowledge of isogeny relations and a family of signature schemes.

The result is a flexible family of post-quantum signature schemes that achieves comparable performance compared to the most advanced isogeny-based signatures available today. Although the signatures themselves are somewhat larger in size, the efficiency gains and solid security foundations make these schemes a compelling approach for future cryptographic standards and applications. Additionally, improvements in polynomial commitment schemes' efficiency immediately translate to efficiency of our signatures.

Proofs of Knowledge of Isogenies

Aside from post-quantum signatures, SPRINT also serves as a proof of knowledge of isogeny relations. These proofs let someone demonstrate that they know an isogeny without revealing it. This ability is important in post-quantum cryptography because many protocols rely on these hidden relationships to function securely. Traditionally, however, these proofs have been slow or required special assumptions, which has limited their practical use. SPRINT also acts as a new proof system that overcomes these obstacles: it uses modern polynomial-commitment techniques to create proofs of isogeny knowledge that are much faster and easier to verify, while relying only on well-understood, standard security assumptions. These proofs can in turn be used to create the mathematical setup needed for other isogeny-based cryptography. This makes SPRINT a promising foundation for the next generation of post-quantum cryptographic schemes.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

www.unibw.de/crypto-en

FIG.: SHUTTERSTOCK / JACKIE NIAM

Prof. Dr. Arno Wacker

Privacy and Compliance

Do not just teach data privacy and compliance, live it!

ONE OF THE MOST important goals of the professorship is not only to research and teach data protection and IT security, but also to live them in everyday life. This is the only way to communicate these topics to students in a convincing and authentic manner. The team members also want to show the general public that privacy-enhancing technologies can be integrated into everyday life, both in private and business contexts.

Teaching

In the professorship, teaching is divided into data protection, privacy-enhancing technologies, pentesting, cryptology, and secure networks and protocols. Data protection and privacy-enhancing technologies teach students, among other things, what privacy is and why it is important both for individuals and for democratic societies. Pentesting covers the testing of individual systems, complex IT services, and entire IT infrastructures, as well as practical attack variants based on established best-practice documentation. Cryptology teaches the fundamentals of cryptography as well as knowledge of the various methods for secure data transmission in modern communication networks.

Research

A particular focus of the professorship is on methods and mechanisms that support privacy and data protection. The research is divided into three areas:

- Privacy-supporting mechanisms aim at strengthening individual privacy and researching communication rules for the Internet age.
- Raising IT security awareness addresses, among other things, the area of self-data protection. To this end, the professorship develops and researches methods and tools to increase security awarenes in the development and use of software tools.

Digital security and data protection are core areas of research and teaching at the professorship.

- Cryptanalysis of classical ciphers examines classical encryption methods using modern (meta-)heuristic approaches, focusing on the efficiency of analyses and the security of the algorithms.

Knowledge Transfer

A key mission of the professorship is to train, educate, and inform interested members of the public about IT security issues. All team members pursue this goal through lectures and workshops on topics such as pentesting, secure everyday e-mail communication, and the detection of security vulnerabilities.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

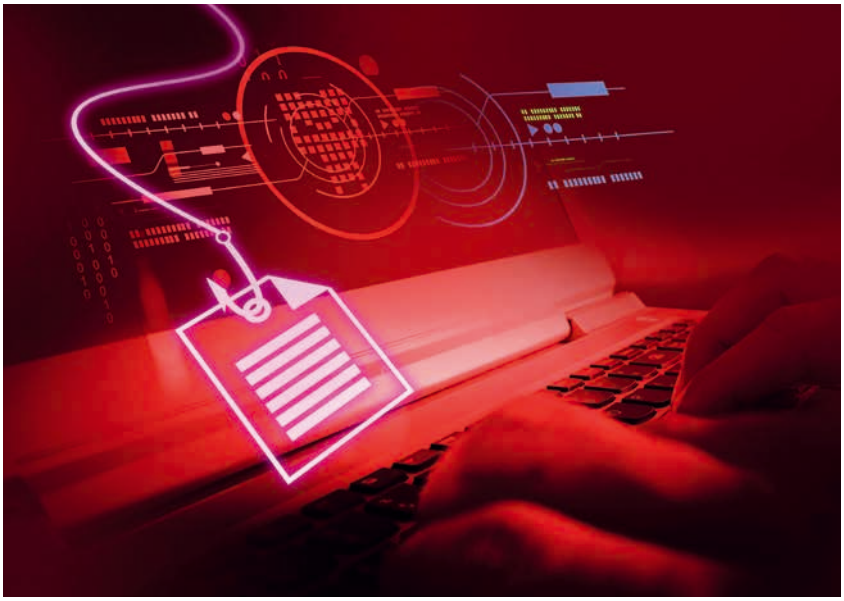
www.unibw.de/datcom

FIG.: ISTOCK / MATEJMO; RI CODE / DATCOM

Expired Domains in Connection with Email Infrastructure

An Empirical Study on Expired Domains Used in Email Infrastructure

This research project deals with an empirical study of past behavior and change patterns of expired email domains and their impact on email infrastructure and security.



Criminals can use legal procedures to buy access to your email communication.

IT IS NOW undeniable that email and the infrastructure on which it is based are an everyday part of both private and professional life. In particular, public authorities and professionals regularly transmit sensitive data that may also be subject to confidentiality obligations. This is especially relevant given the current technological shift from traditional methods such as fax to modern electronic transmission methods such as email.

The scientific community has already pointed out the dangers posed by expired and newly registered domains in various research papers and publications. However, this issue has not yet been empirically investigated. Therefore, this research project focuses on conducting an empirical study to collect datasets and gain new insights that can be used for academic development. Among other things, this may include determining the prevalence of such phenomena.

This is particularly critical because, apart from end-to-end encryption of emails, there is no way to protect against expired or newly registered email domains. An analogy can be drawn with a maibox: when the previous tenant moved out, they removed their nameplate. However, the new tenant or even a third party could, although it is legally prohibited, technically attach the nameplate or a new nameplate with the previous tenant's name and thereby intercept the mail intended for them.

The study draws on public and partially publicly accessible datasets, in particular ICANN's zone files, which list all domains in the corresponding top-level domains. The domains contained in the zone files are further processed so that, among other things, data of the associated email infrastructures (MX records) can be extracted. These MX records are used to contact the relevant email servers and extract information from the cryptographic certificates. This should make it possible to detect whether an email server has changed, for example if the fingerprint of a certificate has changed. However, this method cannot be used to determine whether a change is malicious or benign in nature.

In particular, the findings may be used to implement security mechanisms or standard enhancements to mitigate the risk posed by expired email domains.

Linus Laurenz

linus.laurenz@unibw.de

+49 89 6004-7372

FIG.: ADOBE STOCK / JANEWS094

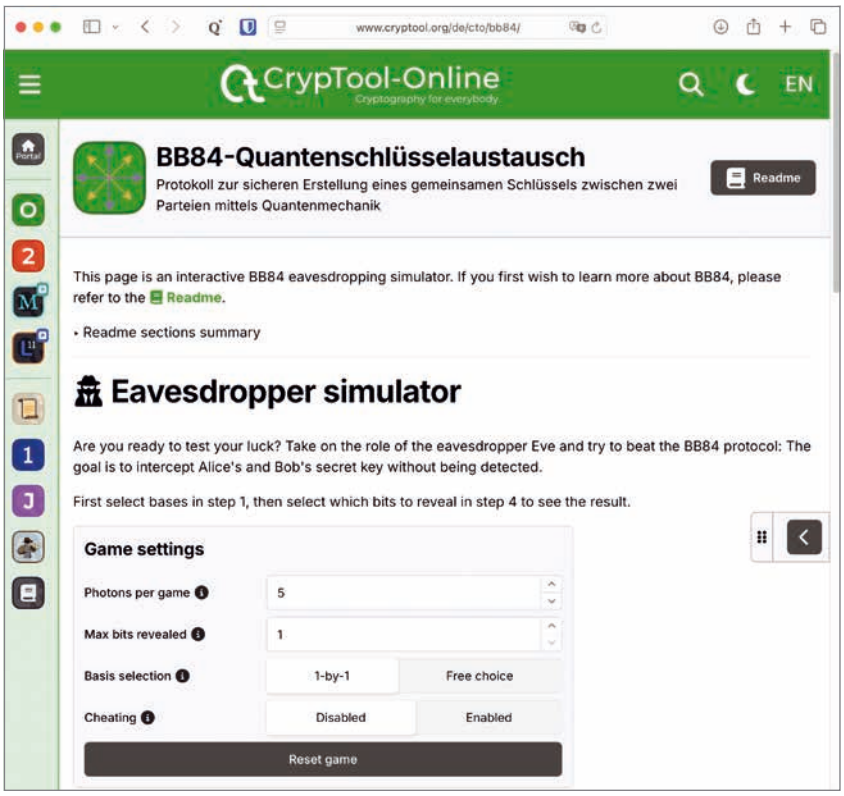
CrypTool

Further Development of the CrypTool Website in 2025

In 2025, the CrypTool website underwent comprehensive technical and functional modernization. The focus was on migrating to a new web framework, introducing additional interactive learning applications (CTO apps), and improving user-friendliness, code quality, and operational reliability.

New Applications and Features

Several apps were newly integrated or revised: Enigma, Base64, Vernam, BB84, Kyber/ML-KEM, and Frequency Analysis. These projects required extensive code review and, in some cases, weeks of additional work to reach production quality. Existing modules such as CryptoBrief, Monoalphabetic Substitution, Railfence/Redefence, and Caesar were also improved in functionality and visualization. The Python integration received an isolated execution context and a new editor with output window.



Web app for the BB84 protocol.

Technical Updates

The frontend framework Next.js was upgraded to version 15, and Chakra UI to version 3 — a complex migration that required numerous adjustments to components, hooks, and styles. The design was completely revised; fonts are now provided locally via "@fontsource", tables and layouts are more responsive, and the homepage was redesigned with a clearer project overview. In addition, the icon library was migrated to Font Awesome 6.

Code Quality and Automation

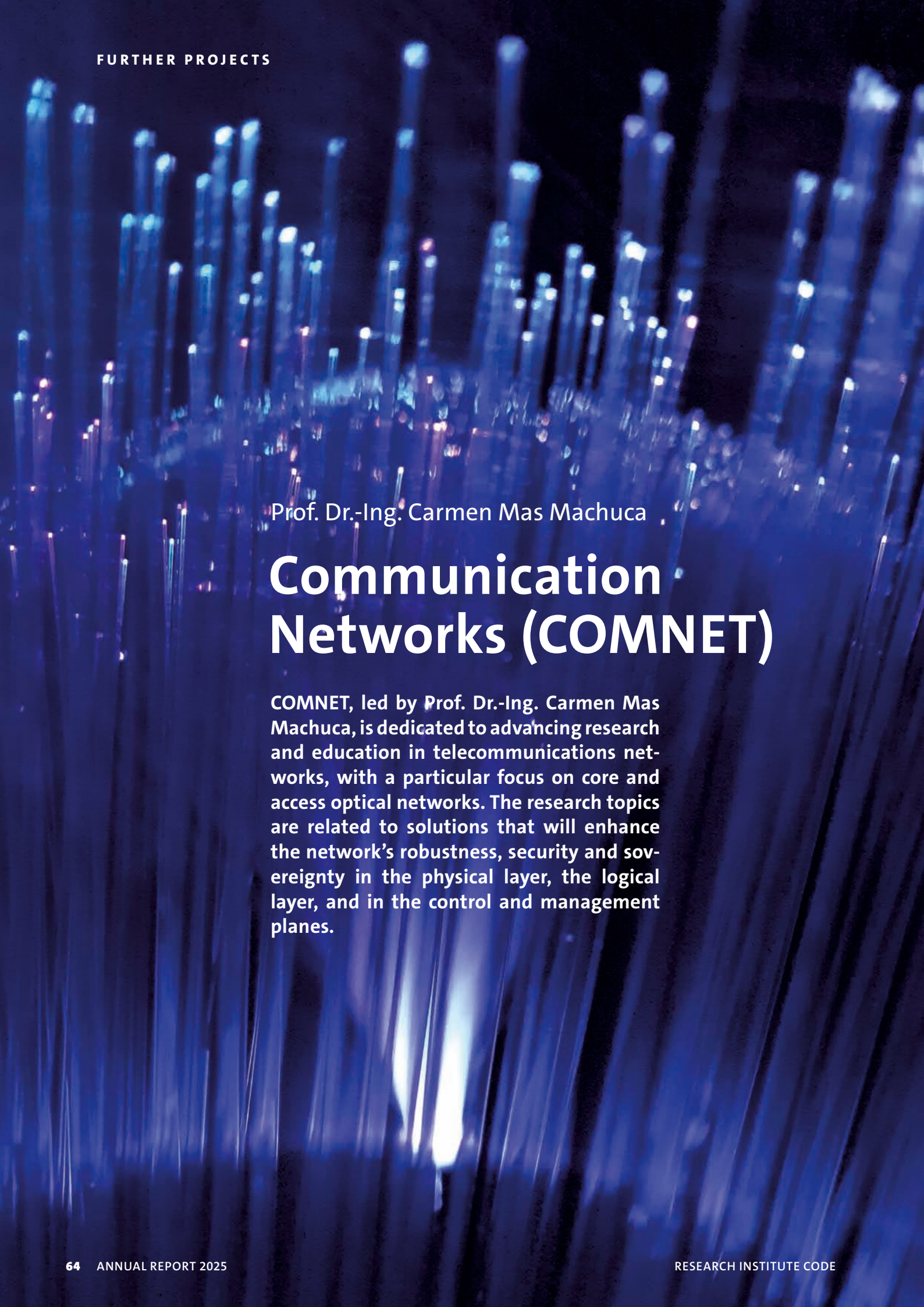
New configurations for Prettier and ESLint ensure consistent formatting and automatic code checks in the CI pipeline. Errors in React hooks and imports are detected early and corrected. A GitHub workflow automates build, release, and deployment processes via webhook — a major efficiency gain in development.

Operations and Infrastructure

The server and network infrastructure were consolidated, mail systems simplified, and reliability improved through redundancy and automatic replication. Download links to JavaCrypTool versions are now cached during the build, preventing API errors during downtime. As a result, a modern, robust, and easily maintainable platform was created, providing the technological foundation for current and future cryptography learning tools — with a unified design, optimized performance, and future-proof architecture.

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

FIG.: CRYPTOOL / DORIS BEHRENDT



Prof. Dr.-Ing. Carmen Mas Machuca

Communication Networks (COMNET)

COMNET, led by Prof. Dr.-Ing. Carmen Mas Machuca, is dedicated to advancing research and education in telecommunications networks, with a particular focus on core and access optical networks. The research topics are related to solutions that will enhance the network's robustness, security and sovereignty in the physical layer, the logical layer, and in the control and management planes.

COMNET was established in April 2023 and is part of the Faculty of Electrical Power Systems and Information Technology. It currently has one post-doc and twelve doctoral candidates (five in campus and seven external, mainly at TUM where Prof. Mas Machuca is currently a Privatdozent). The professorship has four running national BMFTR projects covering topics from access and core networks on network resilience, security, sovereignty, and resource allocation.

Research Topics

Network sovereignty is becoming increasingly important in communication networks, as it guarantees regular operation independently of political, market or planning restrictions. Advancements in standardization allow components from different manufacturers to be interoperable, reducing the problem of vendor lock-in. We investigate the optimal number of manufacturers and the location of their components in order to increase network sovereignty. This area is being investigated in the SUSTAINET-Advance project. In addition, the BMFTR-funded HYPERCORE project is investigating the scalability of optical networks in terms of capacity, reliability, and sovereignty.

The increasing demand for secure communications is encouraging operators to consider deploying QKD on their networks. The research addresses various planning issues with the aim of reducing costs while ensuring secure transmission. Multiperiod planning solutions for investments are provided as required. Furthermore, the distribution and use of exchanged keys are optimized. New approaches to increasing both security and availability have been proposed and are currently being tested in a real system.

Access networks are the last network segment to be protected due to the high deployment cost. Consequently, most current access networks have a tree topology to easily scale with the number of connected users and reduce infrastructure costs. COMNET models, plans and evaluates different protected architectures that can increase connection availability. These topics are addressed in the FRONT-RUNNER project. Furthermore, dependability analyzes are performed to evaluate and reduce the interdependency between the power grid and communication networks, which are addressed in the PONGO project.

Access networks connect end users to the core network, and thus provide access to communication services.

Activities

This year, COMNET participated in the organization of the international ONDM conference as TPC co-chair, and gave invited talks at Optica OECC/PSC 2025 on ‘Towards Resilient and Secure QKD Networks’ and at WueWoWas 2025 on ‘Resilience and Sovereignty Metrics and Models’. Several technical presentations were submitted and accepted at various national and international conferences, including the VDE ITG Conference on Photonic Networks, IEEE EuCNC & 6G Summit, IEEE RNDM 2025, Berlin 6G Conference, IEEE ICTON 2025, WueWoWas 2025, and IEEE FNFW 2025. Some of these presentations received awards for the best paper: e.g., the paper ‘Routing, Band, Modulation, and Spectrum Assignment with Dedicated Protection in Multiband-Elastic Optical Networks’ presented by Dr.-Ing. Anjali Sharma at IEEE ONDM 2025, and ‘Investigating the Correlation Between Minimal Cut Set and Flow Availabilities’ presented by Shakthivelu Janardhanan at WueWoWas 2025. The group has also given demonstrations at the IEEE EuCNC & 6G Summit, the Berlin 6G Conference, and the IEEE ICTON.

Prof. Dr.-Ing. Carmen Mas Machuca

cmas@unibw.de

+49 89 6004 7560

www.unibw.de/comnet

FIG.: AIRBUS HELICOPTERS / CHRISTIAN KELLER; AMIUS REPORT

Juniorprof. Dr. Maximilian Moll

Operations Research — Prescriptive Analytics

Juniorprof. Moll's research focuses, on the one hand, on reinforcement learning, where he is particularly interested in the possible combinations with classical operations research as well as the applications in prescriptive analytics and prescriptive intelligence. On the other hand, he is researching the interfaces of quantum computing with optimization and machine learning.

Data-driven Monitoring of Land Systems

Spare Parts Forecast for the GTK Boxer Weapon System

The project supports the operational readiness of the German Armed Forces' land systems: Combined and adjusted GTK Boxer data from various data sources is used to forecast spare parts demand during maintenance measures. The results are automated spare parts packages and visualizations with clear key performance indicators. In the future, decision-makers will be able to access these by making them available on pCloudBw.

MATERIAL READINESS is a key concern for the German Armed Forces. The growing volume of telemetric, logistical, and usage-related data opens up new opportunities to assess the condition of land systems early on and to provide spare parts in a targeted manner. This project therefore aims to further develop the methodology for data-based monitoring of land systems. In addition to investigating sensor technology in other subprojects, the data already collected on usage profiles and spare parts consumption from various data sources will be fused and evaluated for the GTK Boxer. Thus, the project is not only of direct importance to those responsible in the German Armed Forces, but also offers scientific innovation potential in spare parts forecasting.

Interior view of a GTK Boxer.

Challenge: Database

The existing demand data contains numerous attributes in which descriptions have been formulated individually. These varying designations lead to inconsistencies, which must first be resolved through comprehensive cleanup. In the further course of the project, the cleaned inventory data will then be merged with usage and sensor information.

Advanced Spare Parts Forecasting

The project is divided into two core pillars. On the one hand, innovative approaches to spare parts forecasting are being developed. The project distinguishes between plannable replacement intervals and unplanned damage events. For the first case, a procedure is being developed to identify suitable replacement packages and optimally coordinate their delivery times. In the second case, detailed usage profiles—such as driving distances, terrain characteristics, and load levels—are incorporated into a learning model that forecasts the probability of future defects.

Operationalization and Visual Decision Support

Secondly, these results should not remain theoretical, but should be made usable in practice. To this end, the models are prepared in such a way that they can be seamlessly integrated into automated data pipelines. The project is thus one of the first to use the Bundeswehr's new pCloudBw infrastructure for such applications and to add essential functionalities to the Bundeswehr's large equipment forecasting capability project from the Analytics and Simulation cluster program. At the same time, advanced visual decision support is being developed: a web interface provides those responsible for procurement, maintenance, and deployment planning with clear performance indicators. This enables decisions to be made in a data-driven, transparent, and timely manner.

Juniorprof. Dr. Maximilian Moll

maximilian.moll@unibw.de

+49 89 6004 2248

www.unibw.de/comtessa-en

FIG.: ADOBE STOCK / TIERNEY; BUNDESWEHR / MANDT

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

The Artificial Intelligence and Machine Learning (AIML) group, led by Prof. Dr. Eirini Ntoutsi, develops AI systems that are *technically robust* - meaning resilient to real-world data challenges such as bias, data imbalance, distribution shifts, and adversarial attacks - and *societally responsible*, with emphasis on fairness, explainability, and accountability ensuring traceable and auditable AI decisions.

DZdA – German Center for Digital Tasks in Higher Education Teaching

Generative AI-supported Digital Task Creation and Assessment to Improve Learning Outcomes in Higher Education

The DZdA project establishes the German Center for Digital Tasks in Higher Education Teaching to support AI-based digital task creation, assessment, and sharing across institutions. Advances in generative AI enable adaptive assessment and new forms of educational content, improving learning outcomes through targeted task generation, automated evaluation, and personalized learning recommendations.

Background and Motivation

Digital teaching and assessment have evolved rapidly in recent years, driven by advances in digital platforms and generative AI models. While these models show strong capabilities in specific contexts, such as summarization and feedback support, their performance across disciplines, task types, and educational objectives remains insufficiently understood, raising questions of reliability, consistency and pedagogical suitability. At the same time, the development and sharing of high-quality digital tasks remains fragmented and institution-specific, limiting scalability in higher education.

Project Vision and Objectives

The DZdA project addresses this gap by establishing a national center for digital tasks in higher education teaching. Its overarching goal is to enable the creation, assessment, and sustainable sharing of high-quality digital tasks across institutions. By providing a structured infrastructure and community-driven services, DZdA aims to improve teaching quality, foster reuse of validated tasks, and support scalable and adaptive assessment practices across disciplines.

AI-supported digital assessment and learning in higher education.

Role of the AI & Innovation Center

A central pillar of the DZdA is the AI & Innovation Center, led by the AIML group. The center is responsible for developing and integrating AI-based methods that support task creation, assessment, and intelligent learner support. This includes AI-assisted task generation, automated evaluation, and the development of mechanisms for personalized learning recommendations. A key focus is the responsible and transparent use of generative AI, ensuring reliability, robustness, and pedagogical appropriateness. The center addresses the challenge of generating high-quality tasks across multiple objectives and contexts, as well as the multi-dimensional evaluation of AI-generated tasks, recommendations, and explanations for learners and instructors.

Progress and Outlook

In the initial phase, the project focuses on the systematic evaluation of both generic and education-specific foundation models across multiple learning-relevant dimensions. This includes assessing model performance with respect to task quality, feedback accuracy, robustness, alignment with learning objectives, and pedagogical suitability across different disciplines and task types. Based on these evaluations, a carefully selected model or pool of models will serve as a backbone for the approach, providing a stable and well-understood foundation for the informed and responsible integration of generative AI into digital assessment workflows.

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

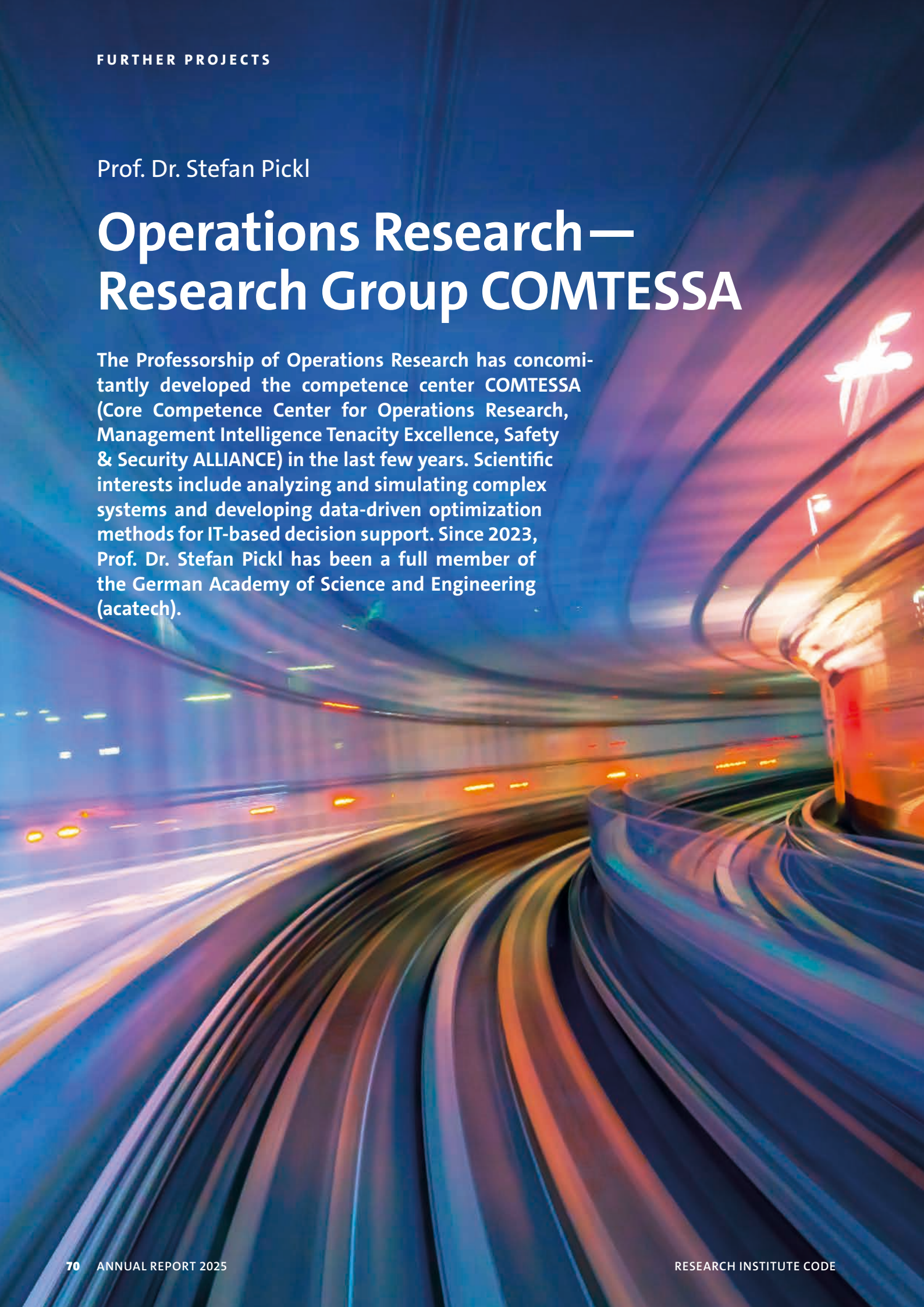
Founded by:
Stiftung Innovation in der Hochschullehre

FIG.: ADOBE STOCK / LUCEGRAFIAR; ADOBE STOCK / ANTONY WEERUT

Prof. Dr. Stefan Pickl

Operations Research — Research Group COMTESSA

The Professorship of Operations Research has concomitantly developed the competence center COMTESSA (Core Competence Center for Operations Research, Management Intelligence Tenacity Excellence, Safety & Security ALLIANCE) in the last few years. Scientific interests include analyzing and simulating complex systems and developing data-driven optimization methods for IT-based decision support. Since 2023, Prof. Dr. Stefan Pickl has been a full member of the German Academy of Science and Engineering (acatech).



REAVRS

Revealing Existing Attack Vulnerabilities in the Rail System

Based on the increasing use of digitalization aspects such as big data, IT, etc., the railroad system has an increased vulnerability to attacks from third parties. A general approach to standardized attack security has not yet been established. REAVRS is developing a complex vulnerability model of the rail system in order to subsequently develop intelligent (AI-based) measures against both physical and cyber threats.

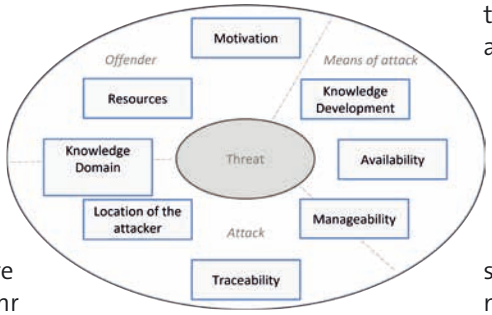
Objective

The objective of the REAVRS research project of the German Center for Rail Transport Research (DZSF) is to determine the current vulnerability of the German railroad system. The participating partners in the project are the University of the Bundeswehr Munich, the COMTESSA research group (project management) in cooperation with the RI CODE, as well as the IVE Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH), CreaLab GmbH, and the Institute of Transport, Railway Construction and Operation (IVE) at the TU Braunschweig.

The project is divided into the following topics:

- Identification of existing attack potentials and scenario development
- Complex root cause analysis
- Intelligent risk analysis and assessment
- Development of recommendations for preventive measures
- Automation of the threat model

As part of the project, an initial identification of existing weaknesses and a comprehensive risk analysis of the causes of these vulnerabilities are carried out. On this basis, security measures and the necessary implementation strategies can be derived and recommended.



Identification of parameters for the threat.

OR-based System Analysis

A functional mapping of the (German) railroad system is developed, followed by precise research into attacks that have occurred and a description of typical contexts. Attack possibilities and threat scenarios are being systematized and a threat identification is created on the basis of an OR-based system analysis.

Cyber Vignettes and Attack Scenarios

After preselecting the points of attack, these are then developed into exemplary model vignettes. When systematizing the means of attack, a general distinction is made between physical vignettes and cyber vignettes. This refers to scenarios that demonstrate how a specific mathematical model or optimization technique is applied to a real-world problem. After extensive research, more than 500 physical and almost 1,000 possible cyber attacks were identified. A selection of representative vignettes is being evaluated. The associated attack scenarios are further described as examples so that a root cause analysis can be carried out. In the final step, the developed methodology is embedded in both a convenient IT-based environment for better decision support as well as in a comfortable management cockpit with reachback functionalities (Comtessa Suite).

Automation and "Safety & Security" Living Lab

The subsequent results of the root cause analysis—the individual values of the respective vignettes—are displayed in a so-called fishbone diagram for selected GSM-R modem cyber vignettes: This detailed root cause analysis is incorporated into the subsequent risk analysis. An automated version of the threat model and a supporting management cockpit are currently being created in order to develop a "Safety & Security" living lab of the German railroad system at HOLM.

Prof. Dr. Stefan Pickl

stefan.pickl@unibw.de

+49 89 6004 2400

https://go.unibw.de/reavrs

Funded by: German Center for Rail Traffic Research (DZSF)

FIG.: ADOBE STOCK / NAKA; PICKL S., BUCHETMANN B., ALONSO VILLOTA M., LORETH T. UNIBW M; SIEFER T., STUTE F. TU BRAUNSCHWEIG.; JELINSKI M. IVE MBH, HANNOVER.; NEUBECKER K. A., SCHMITZ W. CRE-ALAB GMBH, FELDKIRCHEN-WESTERHAM.

Prof. Dr. Corinna Schmitt

Secure Communication Systems

The Secure Communication Systems (SeCoSys) research group investigates secure, privacy-aware communication in complex IoT ecosystems. Its research focuses on resilient networks, trustworthy data management, and cross-domain solutions for connected systems—ranging from aviation to critical infrastructure.

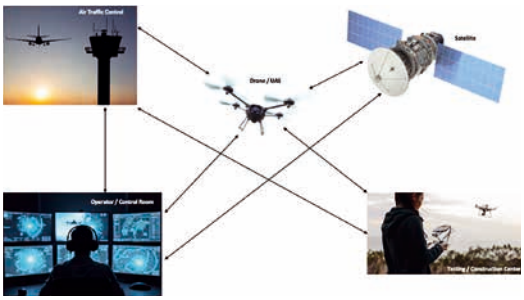
Cyber Resilience in Unmanned Aviation

Standardization of IT Security and Resilience for the Operation of Unmanned Aviation Systems

Unmanned aviation systems (often referred to as "drones") are becoming increasingly important in business, administration, and security organizations. In addition to traditional flight safety, digital risks are also a key concern. The SeCoSys group at RI CODE, together with UAV DACH e.V. in the Competence Group IT Safety & Security and authorities/industry, is driving forward the standardization of IT security measures for UAS and developing practical basic protection profiles for securing networked systems.

UNMANNED aerial systems are now used in a wide range of applications—from logistics tasks and disaster relief operations to security-critical missions for the armed forces and government agencies. In addition to flight and operational safety requirements, this also entails a considerable expansion of digital attack surfaces, as modern UAS are complex and interconnected systems: They interact via radio and network interfaces and process navigation and mission data, exposing them to potential cyber risks. If the firmware, communication channels, or control data fail or are manipulated, not only can operations/deployment be disrupted, but people and property can also be endangered.

The aim of this research by the Secure Communication Systems (SeCoSys) group is to use IT baseline protection profiles to provide a systematic and easily implementable basis for information security in UAS operations. Established standards are used and adapted in a practical manner to the specific characteristics of unmanned aviation. In collaboration with the Competence Group IT Safety & Security of UAV DACH e. V., a European association for unmanned aviation that connects stakeholders from industry, research, and government and creates framework conditions for safe, efficient UAS operations, profiles are being developed that provide concrete recommendations for securing IT components, processes, and responsibilities throughout the life cycle of unmanned systems. To date, two profiles have been developed with the participation of SeCoSys, which are based on the established IT baseline protection approach of the German Federal Office for Information Security (BSI):



Schematic representation of the reference architecture including communication paths

- IT-Grundschutz profile for the operation of UAS Volume 1: UAS operating category „Open", which is aimed at all types of UAS operators and specifies basic requirements for information security when operating open, non-specialized systems.
- IT baseline protection profile for the operation of uncrewed aircraft systems in government agencies and organizations with security responsibilities (BOS), contain supplementary profiles for organizations with security tasks, which are based on the open profile and take specific requirements into account.

The profiles contain reference architectures, hazard and risk analyses, catalogs of measures for technical and organizational security, and information on integrating security processes into existing operating concepts. They address typical vulnerabilities such as inadequate protection of communication interfaces, unprotected firmware updates, lack of logging and monitoring mechanisms, and insufficient authentication procedures.

PD Dr. Corinna Schmitt
corinna.schmitt@unibw.de
+49 89 6004 7314
www.unibw.de/secosys-en

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

FIG.: ADOBE STOCK / RINRADA

Cooperations

Germany and the World

National Partners

The RI CODE is working with 74 partners in 46 cities and municipalities in Germany.

THE COOPERATION WITH other universities, public institutions and companies is part of RI CODE's self-image: We learn with and from our partners and can take the first steps towards implementing our research results in practice.

At the same time, this close exchange ensures that we understand the specific questions and problems of our partners and can consider them from a scientific perspective.

Within Germany, our network is particularly tight-knit. As part of the University of the Bundeswehr Munich, we work with 74 institutions in 46 cities and municipalities nationwide. The focus is on Bavaria and the Munich area, North Rhine-Westphalia, and Hessia. ■

	Partner	Location
1	Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur)	Halle (Saale)
2	Airbus Defence and Space GmbH	Taufkirchen/Manching
3	Akhetonics GmbH	Berlin
4	Bavarian State Office for Information Security (LSI)	Nuremberg
5	Bavarian State Criminal Police Office (BLKA)	Munich
6	Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw)	Koblenz
7	Federal Office for Information Security (BSI)	Bonn
8	Federal Criminal Police Office (BKA)	Wiesbaden/Berlin
9	Federal Office of Languages (BSprA)	Hürth
10	BWI GmbH	Meckenheim
11	Christian-Albrecht University of Kiel (CAU)	Kiel
12	CISPA Helmholtz Center for Information Security	Saarbrücken
13	Cyber Security Operations Centre of the Bundeswehr (CSOCBw)	Euskirchen
14	German Institute for Standardisation (DIN)	Berlin
15	German Aerospace Center (DLR)	Cologne/Oberpfaffenhofen
16	dida Datenschmiede GmbH	Berlin
17	Eberhard Karl University of Tübingen	Tübingen
18	ESG Elektroniksystem- und Logistik-GmbH	Munich
19	FAST-DETECT GmbH	Munich
20	L3S Research Center	Hanover
21	Frankfurt University of Applied Sciences	Frankfurt a. M.
22	Fraunhofer Institute for Digital Media Technology (IDMT)	Ilmenau/Oldenburg
23	Fraunhofer Institute for Computer Graphics Research (IGD)	Darmstadt
24	Friedrich-Alexander University of Erlangen-Nuremberg (FAU)	Erlangen/Nuremberg
25	Bundeswehr Command and Staff College (FüAkBw)	Hamburg
26	Leibniz University Hannover (LUH)	Hanover
27	GSI Helmholtz Centre for Heavy Ion Research	Darmstadt
28	Helmholtz Center Dresden-Rossendorf (HZDR)	Dresden
29	Helmut Schmidt University/University of the Bundeswehr Hamburg (HSU/UniBw H)	Hamburg
30	Hessian State Criminal Police Office (HLKA)	Wiesbaden
31	Hessian Police Headquarters for Technology (HPT)	Wiesbaden
32	Bielefeld University of Applied Sciences and Arts (HSBI)	Bielefeld
33	Bochum University of Applied Sciences	Bochum
34	Darmstadt University of Applied Sciences (h_da)	Darmstadt
35	Hamburg University of Applied Sciences (HAW Hamburg)	Hamburg
36	Berlin University of Applied Sciences (HTW Berlin)	Berlin
37	Berlin School of Economics and Law (HWR Berlin)	Berlin

	Partner	Location
38	IDEMIA Identity & Security Germany AG	Bochum
39	Infineon Technologies AG	Neubiberg
40	Leibniz Institute for New Materials (INM)	Saarbrücken
41	Julius Maximilian University of Würzburg (JMU)	Würzburg
42	Karlsruhe Institute of Technology (KIT)	Karlsruhe
43	State Criminal Police Office Baden-Württemberg (LKA BW)	Stuttgart
44	State Criminal Police Office NRW (LKA NRW)	Düsseldorf
45	District of Bad Kissingen	Bad Kissingen
46	Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities (LRZ)	Garching
47	Ludwig Maximilian University Munich (LMU Munich)	Munich
48	German Navy Headquarters (MarKdo)	Rostock
49	Minol-ZENNER-Gruppe	Leinfelden-Echterdingen
50	MTU Aero Engines AG	Munich
51	National Research Center for Applied Cybersecurity ATHENE	Darmstadt
52	nuix	Frankfurt a. M.
53	OTH Amberg-Weiden	Amberg/Weiden
54	Otto von Guericke University Magdeburg (OVGU)	Magdeburg
55	Munich Police Department	Munich
56	RapidMiner GmbH	Dortmund
57	Rohde & Schwarz GmbH & Co. KG	Munich
58	Ruhr University Bochum (RUB)	Bochum
59	secunet Security Networks AG	Essen
60	Siemens Energy AG	Munich
61	Technical University of Applied Sciences Würzburg-Schweinfurt (THWS)	Würzburg/Schweinfurt
62	Chemnitz University of Technology	Chemnitz
63	Technical University of Darmstadt	Darmstadt
64	Dresden University of Technology (TU Dresden)	Dresden
65	Ilmenau University of Technology (TU Ilmenau)	Ilmenau
66	Technical University of Munich (TUM)	Munich
67	TÜV Informationstechnik GmbH (TÜV IT)	Essen
68	University of Konstanz	Konstanz
69	University of Potsdam	Potsdam
70	German National Research and Education Network	Berlin
71	VISTA Remote Sensing in Geosciences GmbH	Munich
72	Defense Technology Agency for Information Technology and Electronics (WTD 81)	Greding
73	Central Office for Information Technology in the Security Sector (ZITiS)	Munich
74	Bundeswehr Centre for Digitalisation and Cyber and Information Domain Capability Development (ZDigBw)	Bonn

ILLUSTRATION: TAUSENDBLAUWERK.DE

Map legend

1 Location number of partners

Partner locations

Internationality

The RI CODE maintains a large international network. In 2025, employees came from 19 countries. We cooperated with 79 partners in 27 countries.

Employees

Nationality	Total
Austrian	13
Brazilian	1
British	1
Bulgarian	1
Croatian	1
French	2
German	112
Greek	2
Hungarian	1
Indian	8
Indonesian	1
Italian	4
Kosovarian	1
Mexican	1
Netherlandish	1
Polish	1
Slovenian	1
South Korean	2
Spanish	3
Total	**157**

International Cooperation Partners

Country	Partner
Australia	CSIRO Data61
	Royal Melbourne Institute of Technology (RMIT)
Austria	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
	P.SYS Caring Systems
	Software Competence Center Hagenberg
	University of Applied Sciences Campus Vienna
	Paris Lodron University of Salzburg (PLUS)
	Vienna University of Technology

FIG.: ISTOCK / BLUE PLANET STUDIO

Country	Partner
Belgium	KU Leuven
Cyprus	Centre for Social Innovation Ltd. (CSI)
Czech Republic	Center for Environmental and Technology Ethics
	Masaryk University (MU)
Denmark	Technical University of Denmark
Estonia	eu-LISA
Finland	Tampere University
France	ARIADNEXT
	Air and Space Force Academy Research Center (CREA)
	EURECOM
	Telecom SudParis
	Grenoble Alps University (UGA)
Greece	Agroknow IKE
	Athena Research and Innovation Center (ARC)
	Centre for Research and Technology Hellas (CERTH)
	EXUS Software
	Harokopio University of Athens
	IASIS NGO
	University of Athens (UoA)
	Ubitech
	University of Ioannina
	University of Piraeus
Ireland	Trilateral Research Limited Ireland (TRI-IE)
Israel	Ben-Gurion University of the Negev
Italy	Abaco S.p.A.
	Fondazione Bruno Kessler (FBK)
	Univeristy of Bologna
	University of Genoa
	University of Roma Tre
	Univeristy of Trento
	University of Turin
Japan	Kyoto University

Country	Partner
Japan	National Institute of Information and Communications Technology (NICT)
	NTT Social Informatics Laboratories
Liechtenstein	University of Liechtenstein
Luxembourg	University of Luxembourg
Netherlands	Eindhoven University of Technology (TU/e)
	University of Groningen
	University of Twente
New Zealand	University of Auckland
Norway	Norwegian University of Science and Technology (NTUT)
	University of Oslo
Poland	Wroclaw University of Science and Technology (WUST)
Serbia	Foodscale Hub
South Korea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Spain	Association Fòrum Dona Activa 2010
	Autonomous University of Madrid (UAM)
Switzerland	EPFL
	Idiap Research Institute
	University of St. Gallen (HSG)
United Kingdom	Imperial College London
	Trilateral Research Limited UK (TRI-IE)
	University of Sheffield
	University of Surrey
USA	Auburn University, College of Engineering
	Brave Software
	Brown University
	City University New York (CUNY)
	Michigan State University
	Naval Postgraduate School (NPS)
	University of Arizona, College of Engineering

Research Visit from Croatia Strengthens Development of New Cybersecurity Solutions

Between 9th and 15th of November 2025, the Research Institute CODE welcomed a group of researchers from the University of Zagreb and its spin-off company CyberArrange Security Solutions. The guests from Croatia had the opportunity to present their work in the field of automation for cybersecurity exercises and carry on interesting discussions with CODE's staff.

Guests from Croatia during their presentation at RI CODE (f. l. t. r.: Ivan Kovačević, Filip Katulić, Mateo Mamut, and Dora Pavelić)

IT IS A PLEASURE when contacts established during the research projects can be further maintained. More than two years has passed since the first research visit of Dr. Ivan Kovačević, at that time a PhD candidate at the University of Zagreb Faculty of Electrical Engineering and Computing (FER). Based on his research interest and PhD work, Dr. Kovačević founded the deep-tech spin-off company CyberArrange Security Solutions (CASS) in 2023.

Close research collaboration and advisory support of the FER have successfully continued, resulting in 15 research papers published in conferences and journals by the research group. Currently, FER and CASS explore the application of Large Language Models (LLMs) in the training of cybersecurity professionals and develop technologies that will be able to prepare realistic cyber range exercises automatically.

Since FER's and CASS's research on cyber ranges, automatic exercise generation, cybersecu-rity for critical infrastructure overlaps with RI CODE's research areas, there is a mutual interest in deepening and expanding collaboration. Experience of cybersecurity training at RI CODE shows that exercise preparation is a time-consuming process, and therefore there is a need and interest to further explore potentials of such AI supported technologies.

During the one-week visit in November, researchers from Croatia and RI CODE had an opportunity to exchange experiences and knowledge, as well as to conduct exercises and tests in CODE's cyber range. The main educational benefit of the visit was the opportunity to have a closer look on how cybersecurity exercises are being designed and implemented in a cyber range environment, which is a great support for the further development of CASS's technologies.

As a young start-up, CyberArrange has already managed to secure around € 400,000 of funding from competitive grants (e.g. NextGenerationEU instrument) and industry partnerships, which enables the companies' further development and activities. RI CODE as a scientific partner is happy to welcome FER and CASS again in the future and looks forward to further cooperation and exchange opportunities, especially within EU-funded projects

Contact person at RI CODE

Ivana Buntić-Ogor
ivana.buntic-ogor@unibw.de
www.unibw.de/code-en

Contact person at FER

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

Contact person at CASS

Dr. Ivan Kovačević
info@cyberarrange.com
www.cyberarrange.com/en

FIG.: CYBERARRANGE SECURITY SOLUTIONS

German-French Exchange on Quantum Computing

For three weeks, Dr. Wolfgang Gehrke from the Research Institute CODE was a guest at the French École de l'air et de l'espace in Salon-de-Provence. The visit focused on quantum computing as well as on establishing and strengthening joint teaching and cooperation formats between the two institutions.

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

FIG.: RI CODE / W. GEHRKE

AS PART OF A research stay, Dr. Wolfgang Gehrke, laboratory supervisor for quantum computing at the Research Institute CODE of the University of the Bundeswehr Munich, visited the École de l'air et de l'espace in Salon-de-Provence, in southern France, from 22 April to 9 May 2025. He was hosted by the Centre de Recherche de l'École de l'Air (CREA), which also houses the Centre d'Excellence Cyberdéfense Aérospaziale (CEC).

The aim of the visit was to exchange ideas on current developments in quantum computing and to further strengthen Franco-German research cooperation.

During his stay, Dr. Gehrke participated in CREA's "Research Day". Under the theme "Harmonizing sensors, AI, and humans to shape intelligent systems of tomorrow", researchers from academia and industry discussed new approaches to combining sensor technology, artificial intelligence, and human factors in safety-critical applications. Numerous starting points for future cooperation emerged from these discussions.

Another major focus of the visit was academic teaching. Dr. Gehrke delivered a specialist presentation entitled "ZX-calculus as an approach to quantum computing" to researchers at CREA.

In this talk, he introduced modern concepts of quantum computing as well as graphical methods such as the ZX calculus. Building on this, he gave a two-hour guest lecture for officer cadets, which attracted considerable interest.

In addition, Dr. Gehrke presented practical examples of real quantum advantage and discussed with French colleagues the development of a quantum computing curriculum for students at the École de l'air et de l'espace. At the end of the visit, both CREA and CODE reaffirmed their intention to continue the exchange and to expand joint activities in research and teaching beyond the field of quantum computing. ■

FIG.: ADOBE STOCK / HAMDEE

Young Science

Offers and Opportunities

Study Award of the Research Institute CODE 2025

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

Award winner First Lieutenant Justin Svrakic (center) with Prof. Dr. Geralt Siebert, Vice President of UniBw M, Dr. Michael Tagscherer, Group Vice President and CTO of Giesecke+Devrient GmbH, Prof. Dr. Stefan Pickl, Head of the COMTESSA Research Group, and Prof. Dr. Wolfgang Hommel, Executive Director of RI CODE (from left to right).

The Research Institute Cyber Defence and Smart Data (RI CODE), in collaboration with Giesecke+Devrient GmbH, has awarded the CODE Study Award 2025 to Justin Svrakic for his master's thesis. In his thesis, *"Design and Optimization of a Multi-Agent System for Traceable Large Language Model-Driven Decision-Making in Cyber-Physical Systems: TADS,"* the graduate of the master's program in computer science addresses an important issue in current AI-based systems, namely the traceable and rule-compliant decision-making of large language models in mission-critical cyber-physical systems.

LARGE LANGUAGE MODELS show great potential for context-based decision support in many fields of application. At the same time, their probabilistic functioning, lack of transparency, and potential inconsistencies make them difficult to use safely in mission-critical environments. However, it is precisely in these environments that it is essential for decisions to be not only correct, but also verifiable, explainable, and clearly linked to rules and empirical knowledge.

The master's thesis was written in collaboration with Fraunhofer Singapore Research Ltd and involved a stay abroad of several months. In this international research context, the work focused on realistic issues in the field of autonomous systems and mission-critical applications. Close collaboration with the local research team made it possible to examine architectural issues not only theoretically, but also with a view to practical application scenarios.

The core of the thesis is the design of the *Traceable Agentic Decision-Making System (TADS)*. TADS describes a multi-agent architecture that systematically combines case-based reasoning and retrieval-augmented generation and extends these with structured reasoning and verification mechanisms to make the decisions of large language models traceable. In addition to a case- and document-based knowledge base, TADS specifically uses the principle of chain-of-thought to translate decision-making processes into explicit, step-by-step argumentation paths.

In addition, a chain-of-verification is used to systematically check and question these argumentation paths and compare them with formal guidelines and mission specifications. Decisions are thus based not only on previous cases and documented rules, but also on transparently structured and verified reasoning steps.

A central architectural principle is the strict separation of decision generation, validation, and execution. While an agent first generates a proposed solution based on similar cases, a separate evaluation agent checks this proposal against documented rules and operational specifications. If rules are violated, the proposal is iteratively revised until a compliant decision is reached. This means that unvalidated proposals cannot be executed directly at any time.

In addition to the conceptual design, TADS was implemented as a prototype in a simulated environment. In a reconnaissance and surveillance scenario, the extent to which previous decisions influence system behavior and the degree to which the integrated validation loop ensures compliance with guidelines were investigated.

The experimental evaluation shows that historical cases have a measurable influence on decision-making, but at the same time, the architecturally anchored validation does not allow any rule violations. The work thus demonstrates that adaptive decision-making and formal traceability are compatible with each other through appropriate system architecture.

With his master's thesis, Justin Svrakic makes an important research contribution to trustworthy artificial intelligence in the field of cyber defense. The thesis combines theoretical foundations, a clearly structured architectural approach, and a well-founded prototypical implementation, thereby addressing a highly topical and challenging research problem.

The CODE Study Award was presented during the master's graduation ceremony on December 13, 2025, on the campus of the University of the Bundeswehr Munich (UniBw M) by Vice President Prof. Geralt Siebert in the presence of CODE's Executive Director Prof. Wolfgang Hommel, Prof. Stefan Pickl, Head of the COMTESSA research group, and Dr. Michael Tagscherer, Group Vice President and CTO of Giesecke+Devrient GmbH ■

FIG.: UNIBW M / SIEBOLD

Study Awards of the University of the Bundeswehr Munich

EVERY YEAR, THE University of the Bundeswehr Munich awards several study prizes donated by different partners. Since 2018, the RI CODE study award has been given to outstanding Master's graduates with a relevant thesis in the field of cyber defense. The award is funded by Giesecke+Devrient GmbH and endowed with €1,000. ■

Laureates of the last years

Year	Name	Subject of the Thesis
2018	Christian Siegert	Automated detection of vulnerabilities in IT security
2019	Philipp Sammeck	Security analysis of an electronic safe lock
2020	Robert Jurisch-Eckardt	Development of a system to fight cybercrime
2021	Martin Lukner	Synthesizing malware traces for digital forensics
2022	Lars Fuchs	Efficient exploitation of vulnerabilities in telecommunication devices
2023	Hannes Ludwig	An approach to creating adversarial samples
2024	Annika S.	Scenario analysis as part of the NEWSROOM project
2025	Justin Svrakic	Design and Optimization of a Multi-Agent System for Traceable Large Language Model-Driven Decision-Making in Cyber-Physical Systems: TADS

Studying at the Research Institute CODE

The **Master's program** in Cyber Security at the RI CODE of the University of the Bundeswehr Munich covers information processing—including planning, formal modeling, implementation, and deployment—with a focus on technical and organizational information security. In addition to well-founded theoretical methods, practical skills are taught, e.g., such as the identification and elimination of security-relevant vulnerabilities, the development and implementation of security concepts, and the detection and mitigation of attacks on IT systems. In addition, legal and ethical issues as well as selected topics concerning the human factor in information security are covered.

The Bundeswehr supports civilian students with a **scholarship for the Master's program in Cyber Security** at the UniBw M. Requirements for this support are a degree (Bachelor or Diplom (FH)) in the STEM field as well as successful participation in a selection process conducted by the Assessment Center for Senior Officers of the Bundeswehr. Besides study programs at a level of excellence and an outstanding level of supervision by teaching staff, the UniBw M offers its students a wide range of leisure activities and amenities. Affordable housing options in one of Germany's most livable and diverse cities complete the benefits.

Further Information

Master's program Cyber Security:
https://go.unibw.de/mcyb
(in German)

Scholarship of the Bundeswehr:
https://go.unibw.de/stipendium-mcyb
(in German)

Doctorates 2025

Rudy Milani

"Advanced Automation for Comprehensible Causal Explanations of Reinforcement Learning Agents"

IN RECENT YEARS, the rise in applications of Reinforcement Learning has been fueled by the availability of powerful computational resources and advanced methods, leading to breakthroughs in areas such as autonomous driving, medicine, and finance. However, these advancements often come at the cost of transparency, leading to diminished trust from human users. Rudy Milani's thesis addresses this issue by proposing Auto-BENEDICT, a novel methodology designed to automatically generate causal explanations for the actions of model-free Reinforcement Learning agents. The explanations provided answer to both "Why" and "Why not" questions, increasing the comprehensibility of agent decisions.

Rudy Milani received his doctorate under Juniorprof. Dr. Maximilian Moll in July 2025. He currently works as a research assistant in the COMTESSA research group. ■

FIG.: ADOBE STOCK / AH. GIEL; PRIVAT

Michael Mundt

"On Efficient and Effective Cyber Threat Intelligence-based Mitigation of Data Exfiltration"

THIS WORK IS facing a current pattern of cyber criminals' modus operandi. They exfiltrate sensitive data to later blackmail the victim or reselling the stolen data, or both. We present a concept to protect against the theft of sensitive data. We investigate methods to become aware of the current cyber threats, show how it can be procedurally integrated into an existing Information Security Management System and investigate the structure of a simulation cycle. The approach is to simulate the attack vector, before an attacker runs it. We consider the interactions between Operational Technology and Information Technology. We evaluated that our approach can be used within valid limits of European regulation. Finally, we provided proof of feasibility.

Michael Mundt received his doctorate under Prof. Dr. Harald Baier in April 2025. He currently works at the Esri Deutschland GmbH and is serving as a visiting scholar at the Professorship of Digital Forensics. ■

Philipp J. Rösch

"Enhancing Conceptual Understanding in Vision-Language Models"

VISION-LANGUAGE (VL) models combine images and text but regularly fail when it comes to concepts such as spatial relationships, color assignments, and sizes of objects. This dissertation addresses this deficit with a concept-specific approach. A positional pre-training and a hard negative contrastive learning framework is introduced, which forces models to learn more complex relationships. In addition, a new benchmark dataset is presented. The results demonstrate a distinct increase in accuracy and, for the first time, offer a method for precisely integrating diverse concepts into VL applications.

Philipp J. Rösch received his doctorate in June 2025 under Prof. Dr. Michaela Geierhos and is employed as research head of artificial intelligence at the Institute of Distributed Intelligent Systems. ■

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

Sergej Schultenkämper

"Information Disclosure on the Web: Development of a Risk Model for the Digital Twin"

INFORMATION DISCLOSED on the web—no matter how insignificant—can, when combined with other data points, pose a considerable threat and thus significant security risks. The dissertation addresses this problem with a framework that uses data-driven aggregation methods to combine information from different profiles into consistent digital twins. On this basis, a risk model is developed that shows how attractive a person is as a potential target for identity theft and how easily a spear phishing attack can be tailored to them.

Sergej Schultenkämper received his doctorate in October 2025 under Prof. Dr. Michaela Geierhos. Now he works in the Career@BI program as a lecturer for special tasks at HSBI and as a data scientist at wonk.ai GmbH. ■

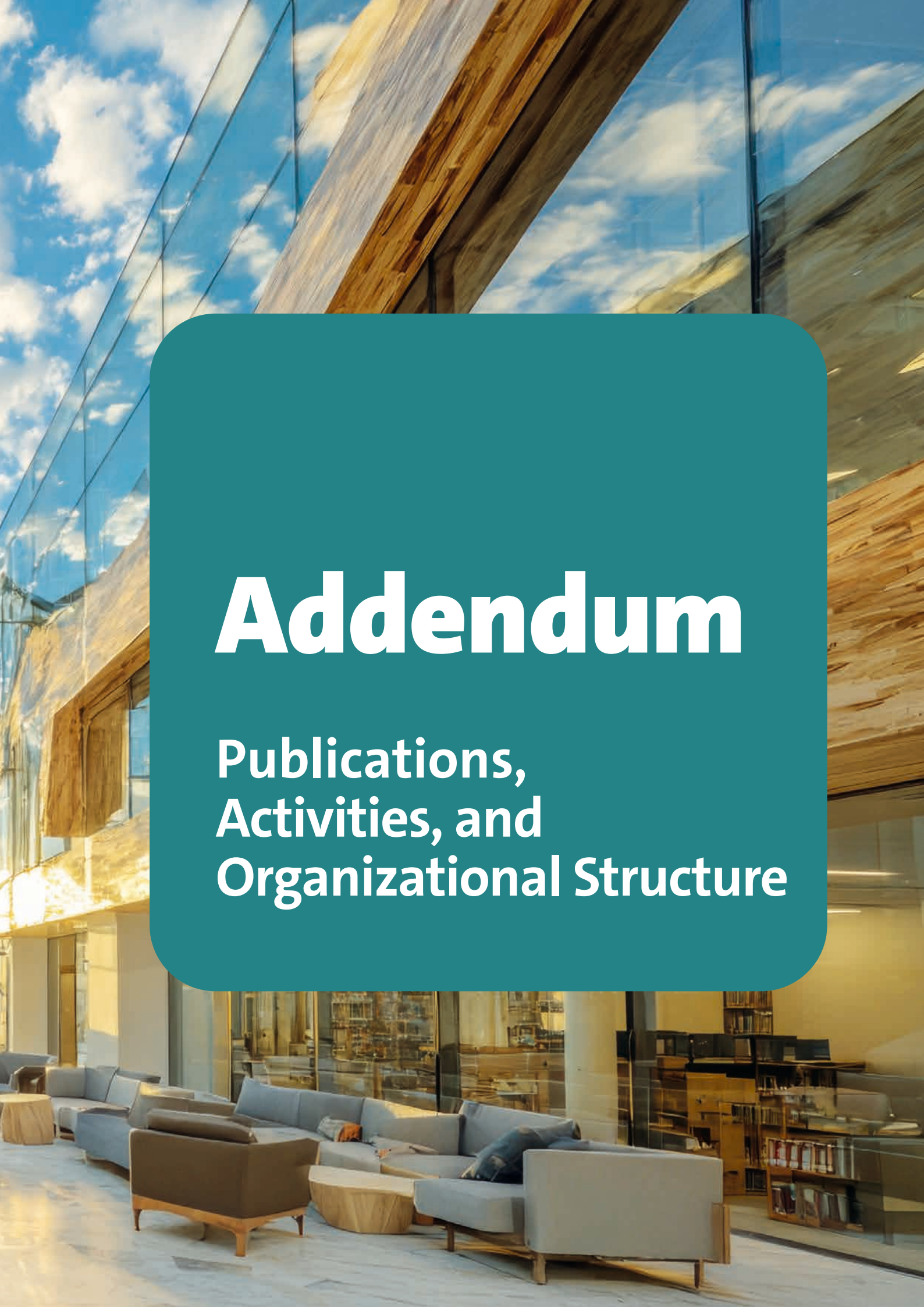
Laura Stojko

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

LARGE INTERACTIVE displays in semi-public areas can be used by many different people, each with their own individual cultural background that influences the user experience of such displays. This dissertation developed a personalization approach that considers the intercultural design preferences of small user groups, preserves privacy requirements through group modeling (aggregation), and enables the display to automatically adapt to groups. A mixed-methods evaluation validated the approach and showed a significant improvement in user experience.

Laura Stojko received her doctorate under Prof. Dr. Michael Koch in August 2025. She is currently a postdoctoral researcher with Prof. Dr. Wolfgang Hommel at the Institute of Software Technology. ■

FIG.: ADOBE STOCK / NAJMA'S VISUAL



Addendum

Publications, Activities, and Organizational Structure

Prof. Dr. Harald Baier

Digital Forensics

PUBLICATIONS

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), pp. 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), pp. 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.

TEACHING

1162	**Advanced Digital Forensics**
3824	**Digital Forensics**
5001/1009	**Seminar Digital Forensics**
5501/1009	**Seminar Forensic Methods in Computer Science**
5505	**IT Forensics**

FAIRS, CONFERENCES, SEMINARS

- Preparation and moderation of the CAST-Workshops Forensik/Internetkriminalität on November 20, 2025, Darmstadt, Germany, URL: https://cast-forum.de/workshops/infos/355
- Talk “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, September 16, 2025, Albstadt, Germany

ADDITIONAL FUNCTIONS

- Chair of the Examination Board for the Master’s Degree Program in Cyber Security at the UniBw M
- Co-Chair of the Technical Programme Committee of the Digital Forensics Research Workshop (DFRWS) USA 2025
- Member of the Faculty Council of Computer Science
- Member of the IT Forensics Expert Committee of the IHK für München und Oberbayern (Chamber of Commerce and Industry)
- Member of the Program Advisory Board for the Master’s Degree Program in Digital Forensics at the Albstadt-Sigmaringen University
- Member of the Steering Committee of the Conference IT Security Incident Management & IT Forensics (IMF), https://www.imf-conference.org
- Member of the Organization Committee of the IMF 2025
- Reviewer for the Journal Digital Investigation
- Reviewer for the Journal Computers & Security

Program Committee

- 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 Doctoral Award 2025
- GI-Skill

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

PUBLICATIONS

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.

RESEARCH PROJECTS

APERITIF — Analysis Pipeline for Effective Vulnerability Identification Through Fuzzing

The goal is to increase the scalability of fuzzing up to datacenter scales, and subsequently perform basic research on novel parallelization and optimization of fuzzers to increase their cov¬erage and, consequently, vulnerability yield.

Funded by: BMVg/BAAINBw
Duration: 2021 — 2025

DEMISEC — Detecting Malicious Implants in Source Code

Modern software depends on many external open source components written by many different parties. If the contributions of only one such party are compromised, the securi¬ty of the entire product is at risk. In DEMISEC, the researchers investigate how to detect malicious source code modifications before they can subvert the development process.

Funded by: BMVg/BAAINBw
Duration: 2021 — 2025

DEPS — Dependable Production Environments with Software Security

The DEPS project endeavors to devise a whole family of novel techniques to protect software and intellectual property by binding software to hardware. As a result, neither will regular, known ways to attack software systems be less effective, nor will reverse en-gineering be an effective way to maliciously obtain intellectual property.

Funded by: Austrian Research Promotion Agency (FFG), Software Competence Center Hagenberg
Duration: 2022 — 2025

TEACHING

1009 **Seminar Language-based Security**

1009 **Seminar Optimization of Programming Languages**

1010 **Machine-oriented Programming**

3647 **Compiler Construction**

55071 **Language-based Security**

FAIRS, CONFERENCES, SEMINARS

- 23. Colloquium on Programming Languages in Feldkirchen-Westerham
- 41. Workshop of the GI Fachgruppe Programming Languages in Bad Honnef
- 40. IEEE/ACM International Conference in Automated Software Engineering (ASE)
- 61. Workshop of the 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)

PRIZES UND AWARDS

- ACM SIGSOFT Distinguished Paper Award

ADDITIONAL FUNCTIONS

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

Prof. Dr. Michaela Geierhos

Data Science

PUBLICATIONS

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. pp. 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 pp.

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 pp.

GEIERHOS, M.: Künstliche Intelligenz: Potenziale, Risiken und Regulierung. Vergaberecht - Zeitschrift für das gesamte Vergaberecht (VergabeR). 2025. Nr. VS-Sonderheft 5a/2025. pp. 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. pp 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. pp. 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. pp. 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. pp. 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. pp. 210-217.

RESEARCH PROJECTS

VIKING — Trustworthy Artificial Intelligence for Police Applications

The subproject "Explainability of Trustworthy AI Language Models for Transparent Use in Security Agencies for Text Classification" is dedicated to the research of trustworthy AI methods for text classification within the joint project VIKING.

Funded by: BMFTR
Duration: 01/2022 — 03/2025

TACR — Technical Adaptation of Cyber Ranges for Military Use

This R&T study examines how the needs of Bundeswehr agencies for training facilities for the digital environment, so called cyber ranges, can be met. To this end, various use cases and cyber range products are being tested and evaluated. In addition, scenarios will be developed in a military context and tested in practice in an exercise.

Funded by: BMVg/WTD81
Duration: 10/2023 — 09/2025

KiTIE — Competence in Cooperation for Technology Transfer — Identification and Evaluation of Partners using Patent Information

The project is developing a tool for identifying cooperation partners for non-university research institutions based on patent information. The aim is to enable effective and efficient partner identification in technology transfer and to promote transparent and autonomous participation of all stakeholders.

Funded by: BMFTR
Duration: 02/2023 — 07/2026

NAWI — News Articles and Knowledge

The NAWI project deals with knowledge extraction and modeling from news articles.

Duration: 12/2021 — 11/2026

AI-based Speech Signal Decoder

The goal of this proof-of-concept is to prototype a neural network for decoding existing vocoder data to improve reception quality.

Duration: 09/2021 — 12/2026

AutoTrainer milCR- Automated Training Creation for Military Cyber Ranges

The F&T study examines how cyber range training courses can be developed that are specifically tailored to the needs of the German Armed Forces. The study builds on the results of the CD&E project "Cyber Range Bw" and examines the possibilities for the automated generation of environments and scenarios for cyber ranges used for military purposes. The latest technologies from the fields of infrastructure as code, configuration management, and automation are used. In this context, training scenarios are also created and tested in practical exercises with military personnel.

Funded by: BMVg/WTD81
Duration: 10/2025 — 06/2028

FINEST — AI-supported Language Processing Environment

Machine Translation has made significant progress through the use of Large Language Models (LLMs). However, these models are usually trained on general language data and show deficits when translating highly specialized technical terminology. This is particularly true in safety-critical and technical contexts, where translation errors can have serious consequences. The aim of the project is to optimize LLMs for use in technical translations through domain-specific fine-tuning and to evaluate them systematically. An additional focus lies on the investigation of the influence of anonymization on translation quality.

Funded by: BMVg/WIWeB
Duration: 12/2025 — 12/2028

TEACHING

1144 **Knowledge Discovery in Big Data**

3850 **Natural Language Processing**

3851 **Information Retrieval**

3852 **Data Science Applications**

3853 **Analysis of Unstructured Data**

FAIRS, CONFERENCES, SEMINARS

- Bodensee Business Forum 2025 (Graf-Zeppelin-Haus, Friedrichshafen)
- Conference on "Cybersecurity, Resilience and Sovereignty" (Tutzing Academy for Political Education in cooperation with the German Informatics Society and Initiative D21 e.V.)
- DeepLearn 2025 (University of Maia, Portugal)
- KI@BW 2025 (HSU, Hamburg)

ADDITIONAL FUNCTIONS

- Member of the program committee Master's in Cyber Security
- Project leader of "Deutsche Biographie" of the Historical Commission at the BAdW
- Member of the General Council of the Catholic Academy in Bavaria
- Expert for the European Commission
- Expert for VDI/VDE Innovation + Technik
- Expert for the Austrian Research Promotion Agency (FFG)

Program Committee

- 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

PUBLICATIONS

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.

TEACHING

26681 **Selected Topics in Deep Learning**

42111 **Biometric Recognition**

42112 **Selected topics in Biometric Recognition**

42121 **Deep Learning**

42122 **Selected Topics in Deep Learning for IT-Security**

FAIRS, CONFERENCES, SEMINARS

- 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

ADDITIONAL FUNCTIONS

- General Chair of the International Conference of the Biometrics Special Interest Group (BIOSIG, https://biosig.de/)
- Chair of the BIOSIG special interest group of the Gesellschaft für Informatik (GI)
- Deputy Chair of the European Association for Biometrics (EAB)
- Member of the IARP TC4 Conference Committee, the IEEE Biometrics Council Security and Privacy Technical Committee, and the IEEE Information and Forensics Technical Committee
- Delegate of the German Institute for Standardization (DIN) in ISO/IEC SC37 JTC1 SC37 on biometrics
- Co-Affiliation Norwegian University of Science and Technology (NTNU)

Prof. Dr. Wolfgang Hommel

Software and Data Security

PUBLICATIONS

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. pp. 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. pp. 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. pp. 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. pp. 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. pp. 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. p. 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. pp. 317-321.

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

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. p. 12.

RESEARCH PROJECTS

6G-life

With the completion of the first phase of the 6G-life project, a holistic research approach was successfully implemented, within which innovative concepts in scalable communication, novel methodologies, flexible software architectures, and adaptive hardware were developed. The research activities promoted the fundamental idea of human-machine collaboration, while requirements regarding latency, resilience, security, and sustainability were addressed in parallel as multidisciplinary topics.

Funded by: German Federal Ministry of Research, Technology and Space (BMFTR) (subcontracted by TU Munich)
Duration: 12/2022 — 08/2025

ACSE LTE — Airborne Cybersecurity Enhancement Long Term Evolution

Airborne Cybersecurity Enhancement (ACSE) LTE (Long Term Evolution) is the successor to the ACSE project that concluded at end of 2023. As its predecessor, ACSE LTE was a research cooperation between FI CODE and Airbus Defence and Space. The focus of this project was the application of insights gained during the previous project regarding secure aircraft communication to tactical data links.

Funded by: Airbus Defence and Space
Duration: 01/2024 — 12/2025

Application-oriented technology potential for cyber/IT

The goal of the R&T measure "Application-oriented technology potential for cyber/IT" is to identify research ideas and innovations, to bring together diverging interests, goals, and methods in the area of cybersecurity and cyberdefense research, and to promote cross-sector cooperation in the area of technology monitoring in cybersecurity.

Funded by: Bundeswehr Technical Center for Information Technology and Electronics (WTD 81)
Duration: 07/2024 — 12/2026

AutoTrainer milCR — Automated training creation for military cyber ranges

The F&T study Automated Training Creation for Military Cyber Ranges examines how cyber range training courses can be developed specifically tailored to the needs of the German Armed Forces. The study builds on the results of the CD&E project "Cyber Range Bw" and examines the possibilities for the automated generation of environments and scenarios for military cyber ranges. The latest technologies from the fields of infrastructure as code, configuration management, and

automation are used. In this context, training scenarios are also created and tested in practical exercises with military personnel.

Funded by: WTD81
Duration: 10/2025 — 06/2028

DEFINE — DC-Grids for reliable power supply

Modern power grids rely heavily on information and communication technologies and cannot be operated without them. However, every IT component offers attack vectors in cyber space, which must be kept as small as possible. FI CODE currently researches approaches for automated attack detection on the communication infrastructure of power grids, in order to guarantee their reliable operation.

Funded by: dtec.bw — Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union — Next Generation EU.
Duration: 01/2021 — 12/2026

Development and integration of real cyber security incidents into cyber range training

In order to respond to the growing threat of cyber attacks, effective training of incident response and forensic specialists is crucial. Cyber ranges offer a secure environment for simulating cyber security incidents. This allows technical skills, tools, processes and roles to be tested without involving real systems and incidents. The aim of this project is to develop a concept that enables the systematic transfer of real cyber security incidents into this training environment.

Funded by: State Office for Information Security (LSI)
Duration: 05/2025 — 06/2028

LIONS — Ledger Innovation and Operation Network for Sovereignty

The project LIONS builds a research platform for enhancing the resilience and digital sovereignty of digitalization using distributed ledger technologies. As part of the inter-disciplinary research project, the research group focuses on the topic of self-sovereign identity management and the technical support of project partners.

Funded by: dtec.bw
Duration: 01/2021 — 12/2026

MuQuaNet — The Quantum Network in the Greater Munich Area

In the MuQuaNet project, a test and demonstration network for quantum communication is being established in the Greater Munich area. The goal is to research technologies for secure key distribution using Quantum Key Distribution (QKD) and to seamlessly integrate them into existing infrastructures. Commercial systems are being tested, miniaturized components developed, and management as well as security mechanisms for future scalable quantum networks implemented.

Funded by: dtec.bw
Duration: 10/2020 — 12/2026

ROLORAN — Resilient Operation of LoRa Networks

As a long-range, energy-efficient radio technology, LoRaWAN offers a promising basis for stable long-range communication. This project investigates the robustness and limits of LoRaWAN through experimental and theoretical analyses, supports protocol security through software hardening and demonstrates the applicability by developing selected prototypes and setting up exemplary IoT infrastructures.

Funded by: dtec.bw
Duration: 01/2021 — 12/2026

TACR — Technical Adaptation of Cyber Ranges for military use

The R&T study Technical Adaptation of Cyber Ranges for Military Use examined how the needs of Bundeswehr agencies for training facilities for the digital environment, so-called cyber ranges, can be met. To this end, various use cases and cyber range products were being tested and evaluated. In addition, scenarios were developed in a military context and tested in practice in an exercise.

Funded by: WTD81
Duration: 10/2023 — 06/2025

TEACHING

1006 **Introduction to Computer Science 1**

1007 **Introduction to Computer Science 2**

1640 **Identity Management (PD Pöhn)**

1785 **IT Security (PD Pöhn)**

3459 **Selected Chapters of IT Security**

3479 **Cyber Security Methods (PD Pöhn)**

5501 **Seminar Application and Software Security**

5501 **Seminar Information Security Managemen**

5507 **Secure Networked Applications**

5508 **Information Security Management**

FAIRS, CONFERENCES, SEMINARS

- Workshop Chair EDId @ ARES 2025 (PD Pöhn)
- Workshop Chair OID 2025 (PD Pöhn)
- DKE BKT Meeting Frankfurt (PD Pöhn)
- ABIS Workshop at the Mensch und Computer 2025 (Dr. Stojko)

ADDITIONAL FUNKTIONS

- Dean of the Computer Science department
- Member of the Operating Committee of the German Research and Education Network

Program Commitee

- IEEE/IFIP International Symposium on Integrated Network Management
- IEEE/IFIP Network Operations and Management Symposium
- DFN Conference Security in Networked Systems
- 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

PUBLICATIONS

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.

RESEARCH PROJECTS

SCANDIUM

The project explores ways of improving cooperation between German law enforcement agencies facing complex, resource-intensive investigative tasks. While these agencies are willing to collaborate, strict regulations prevent them from sharing sensitive information directly. Therefore, coordination must be achieved in a way that respects confidentiality while enabling the efficient use of limited resources.

Fundey by: Central Office for Information Technology in the Security Sector (ZITiS)
Duration: 08/2025 — 07/2028

LIONS — Ledger Innovation and Operation Network for Sovereignty

The interdisciplinary research project is developing a platform for investigating distributed ledger technology as a digitalization technology to increase resilience and digital sovereignty. This includes the further development of distributed and sovereign identity management under security and protection aspects in application areas such as IoT, web applications and eGovernance.

Funded by: dtec.bw — Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union — Next Generation EU.
Duration: 01/2025 — 12/2026

TEACHING

55481 **Modern Cryptography**

55482 **Research Trends in Cryptography**

55631 **Private Data Processing**

55632 **Private Authentication and Messaging**

55633 **Seminar Privacy Enhancing Cryptography in Practice**

FAIRS, CONFERENCES, SEMINARS

- Dagstuhl-Seminar “Guardians of the Galaxy: Protecting Space Systems from Cyber Threats” (Invited participant)
- ACNS 2025 (Workshop Chair)
- ACM ASIACCS 2025 (Speaker)

ADDITIONAL FUNKTIONS

- Associate Editor für IEEE Transactions on Information Forensics and Security (IEEE TIFS)
- Associate Editor für International Journal of Information Security (IJIS), Springer
- Visiting Professor at the University of Surrey, UK

Prof. Dr.-Ing. Carmen Mas Machuca

Communication Networks (COMNET)

PUBLICATIONS

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. pp. 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. pp. 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. pp. 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. pp. 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. pp. 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. p. W1J. 6.

RESEARCH PROJECTS

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

The planned project makes a significant contribution to achieving the funding policy objectives of the 'Resilience — Resilient Digital Systems' funding measure by increasing the resilience of optical access networks against external and internal interference using automated processes.

Funded by: BMFTR
Duration: 01/2023 — 12/2025

PONGO — Next-generation passive optical networks

The contribution of the group is on the design and development of a new planning tool that will support the cost assessment of the proposed solutions and will be extended to determine the best migration path given the current optical access networks.

Funded by: BMFTR
Duration: 06/2024 — 05/2027

HyperCORE

The project aims to investigate technologies for increasing transmission capacity, taking into account all three available physical dimensions — time (channel data rates), frequency (channel wavelengths) and space (number of spatial channels) — and optimising them in terms of energy efficiency.

Funded by: BMFTR
Duration: 07/2024 — 06/2027

SUSTAINET-Advance

COMNET aims to contribute towards modeling, implementing, and evaluating resilient networks. Resilience considers not only failures of the communication network itself but also failures of other infrastructures, such as power grids. The interdependencies between the two networks are taken into account to propose new architectures and solutions.

Funded by: BMFTR
Duration: 07/2024 — 06/2027

TEACHING

4088 **Communication Networks I**

4138 **Communication Networks II**

4140 **Photonic Networks**

ADDITIONAL FUNKTIONS

- 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

PUBLICATIONS

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

RESEARCH PROJECTS

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

The NATO working group is investigating the potential of quantum computing for military applications, particularly for processing and evaluating sensor data. The focus is on quantum algorithms for optimisation, machine learning and data analysis in order to improve situational awareness and accelerate decision-making processes.

Duration: 04/2024 — 04/2027

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

The Research Task Group investigates how Reinforcement Learning and Approximate Dynamic Programming can enhance defence and security decision making within NATO. Experts from government, military, and academia collaborate to survey existing RL efforts, develop a guiding framework for RL-based decision support, and derive best practices. The group also formulates recommendations to shape future research and follow-on NATO Science and Technology Organization activities.

Duration: 02/2023 — 05/2026

TEACHING

2031-V2 **Mathematics for administrative computer scientists**

10362 **Operations Research**

14901 **Selected chapters of operations research and decision theory**

29941 **Selected chapters from Data-driven Optimisation**

29942 **Quantum Machine Learning & Optimization**

33961 **Data mining and IT-based decision support**

552611 **Digitalisation**

FAIRS, CONFERENCES, SEMINARS

- GOR-Working Group Simulation and Optimisation of Complex Systems, November 6-7, 2025
- The International Conference on Operations Research 2025 (OR2025) Stream: Simulation and Quantum Computing, September 2-5, 2025

ADDITIONAL FUNKTIONS

- Fellow of the Bavarian Science Alliance for Peace, Conflict and Security Research
- Coordinator for the program for highly talented students at the University of the Federal Armed Forces Munich
- Working Group Leader “Simulation and Optimization of Complex Systems”, German Operations Research Society

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

PUBLICATIONS

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.

RESEARCH PROJECTS

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

Development of a Knowledge Lake Management System (KLMS) to support FAIR and AI-ready data through data quality assessment, bias detection, and explainability, validated in real-world agrifood use cases.

Funded by: European Union (Horizon Europe, HORIZON-CL4-2021-DATA-01-03)
Duration: 09/2022 — 08/2025

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

Research on fairness-aware AI methods addressing multi-discrimination across multiple protected attributes in tabular, network, and multimodal data, with pilot applications in finance, identity verification, and academic networks.

Funded by: European Union (Horizon Europe, HORIZON-CL4-2021-HUMAN-01)
Duration: 11/2022 — 10/2025

TEACHING

2319 **Artificial Intelligence**

2320 **Responsible Artificial Intelligence**

2321 **Machine Learning**

FAIRS, CONFERENCES, SEMINARS

- Organizer, BIAS workshop co-located with the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD 2025).
- Invited Speaker, Brussels Responsible AI Network (BRAIN) Forum: Tackling Multi-dimensional Discrimination in AI.
- Instructor, AIDA PhD Summer School: Advanced course on Bias in AI Systems, Thessaloniki, Grece.
- Keynote Speaker, CISUC, Coimbra, Portugal: Bias and Fairness in AI — Current and Future Trends.
- Invited Speaker, AI Fairness Cluster Meeting, Brussels: The Multifaceted Nature of Bias in AI — Implications for Generalization, Fairness, and Robustness.
- Panellist, Munich Security Conference 2025 Side Event "Automating Human Security - Rethinking the Role of AI in Conflict for the Protection of Civilians", Munich.
- Invited Speaker, TRANSFERleben Breakfast Club 2025, Munich: Towards Trustworthy AI: Technically Robust and Socially Responsible.

ADDITIONAL FUNKTIONS

- Program Committee Member, Master's Program in Cyber Security, UniBw M.
- Board Member and Faculty Representative, Council of Computer Science Faculties at German Universities (Fakultätentag Informatik, FTI)
- Member, L3S Research Center, Leibniz University Hannover
- Member of the Advisory Board, Weizenbaum Institute, Berlin
- Expert Reviewer, European Commission
- Expert Reviewer, Luxembourg National Research Fund
- Member of appointment and hiring committees, UniBw M, and national and international institutions.
- PhD Committee Member, UniBw M and national and international institutions
- Mentor, MENTality Program, UniBw M
- Program Committee Member, international conferences in artificial intelligence and machine learning (including IJCAI, AAAI, ECML PKDD, PAKDD, and FAccT)
- Member: IEEE; ACM; AAAI, GI.

Prof. Dr. Stefan Pickl

Operations Research — Research Group COMTESSA

TEACHING

10245 **Operations Research Lab — Decision Support**

10252 **Seminar Operations Research I**

10371 **Introduction to Business Information Systems**

10372 **Principles of Information and Communication Technology**

10401/2 **Introduction to Business Intelligence**

12311 **Data Mining and IT-based Decision Support**

12325 **Operations Research Lab — Decision Support II**

12326 **Selected Chapters of Operations Research Seminar II**

2038-V1 **AI and Data-driven Optimization**

3481-V1 **Data Science and Analytics**

ADDITIONAL FUNCTIONS

- Vice-President German Committee on Disaster Prevention
- Chair of the Advisory Board German Operations Research Society
- Member DEU NATO SAS Panel
- Member Munich Aerospace
- Member Board of Trustees Hessian Academy of Highly Gifted Pupils
- Steering Committee VOICE — National Society of IT-Users
- Member German Academy of Technology ACATECH
- Member Club of Rome

Prof. Dr. Daniel Slamanig

Quantum Safe & Advanced Cryptography Lab

PUBLICATIONS

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.

TEACHING

10251 **Seminar Cryptology**

39311 **Introduction to Post-Quantum Cryptography**

39312 **Selected Topics in Post-Quantum Cryptography**

39313 **Post-Quantum Cryptography in Practice**

51181 **Foundations of Distributed Systems and Blockchains**

51182 **Research Topics in Security for Decentralized Systems**

FAIRS, CONFERENCES, SEMINARS

- 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, Spain
- 31st International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2025, Melbourne, Australia
- ArcticCrypt 2025, Longyearbyen, Svalbard, Norway
- CrypTO-Konferenz, Turin, Italy
- 23rd International Conference on Applied Cryptography and Network Security — ACNS 2025, Munich, Germany
- BIRS Workshop “Isogeny Graphs in Cryptography”, Banff, Canada
- Leuven Isogeny Days 6, Leuven, Netherlands
- Young Researcher Crypto Seminar Spring 2025, Konstanz, Germany
- Young Researcher Crypto Seminar Fall 2025, Karlsruhe, Germany
- SQIparty2025 workshop, Lleida, Spain

ADDITIONAL FUNCTIONS

- Reviewer for the Deutsche Forschungsgemeinschaft (DFG)
- 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-Organizer of the International Workshop on Foundations and Applications of Privacy-Enhancing Cryptography — PrivCrypt 2025, Munich, Germany
- Keynote Speaker at the Australian Summer School on Privacy 2025, Sydney, Australia
- Keynote Speaker at the "Workshop on Cryptographic Tools for Blockchains" workshop co-located with EUROCRYPT 2025, Madrid, Spain
- Participation in the Panel Discussion "Post Quantum Cryptography", Webinar Trust in Digital Life (TDL)
- Participation in the Panel Discussion "Bringing Privacy Research to Reality", Australian Summer School on Privacy 2025, Sydney, Australia

Program Committee

- 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

Privacy and Compliance

PUBLICATIONS

BEHRENDT, D., BUSSE, B.: How we use LaTeX in the CrypTool project. TUGboat, vol. 46, no.2, pp. 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, pp. 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, Accepted on 31 May 2025. doi: 10.1145/3746279

HÖLZL, R., KLEINE, S., STEPHAN, F.: Improved lower bounds for strong n-conjectures, J. Aust. Math. Soc. 119:1, pp.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, pp. 449-501, 2025. doi: 10.1017/S0305004125000325

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

TEACHING

3480 **Secure Networks and Protocols**

55011 **Vulnerabilities and Attack Vectors Seminar**

55041 **Data Privacy**

55042 **Privacy Enhancing Technologies**

55061 **Introduction to Cryptography**

55062 **Crypto Analysis**

55091 **Penetration Testing**

55093 **Penetration Testing Lab**

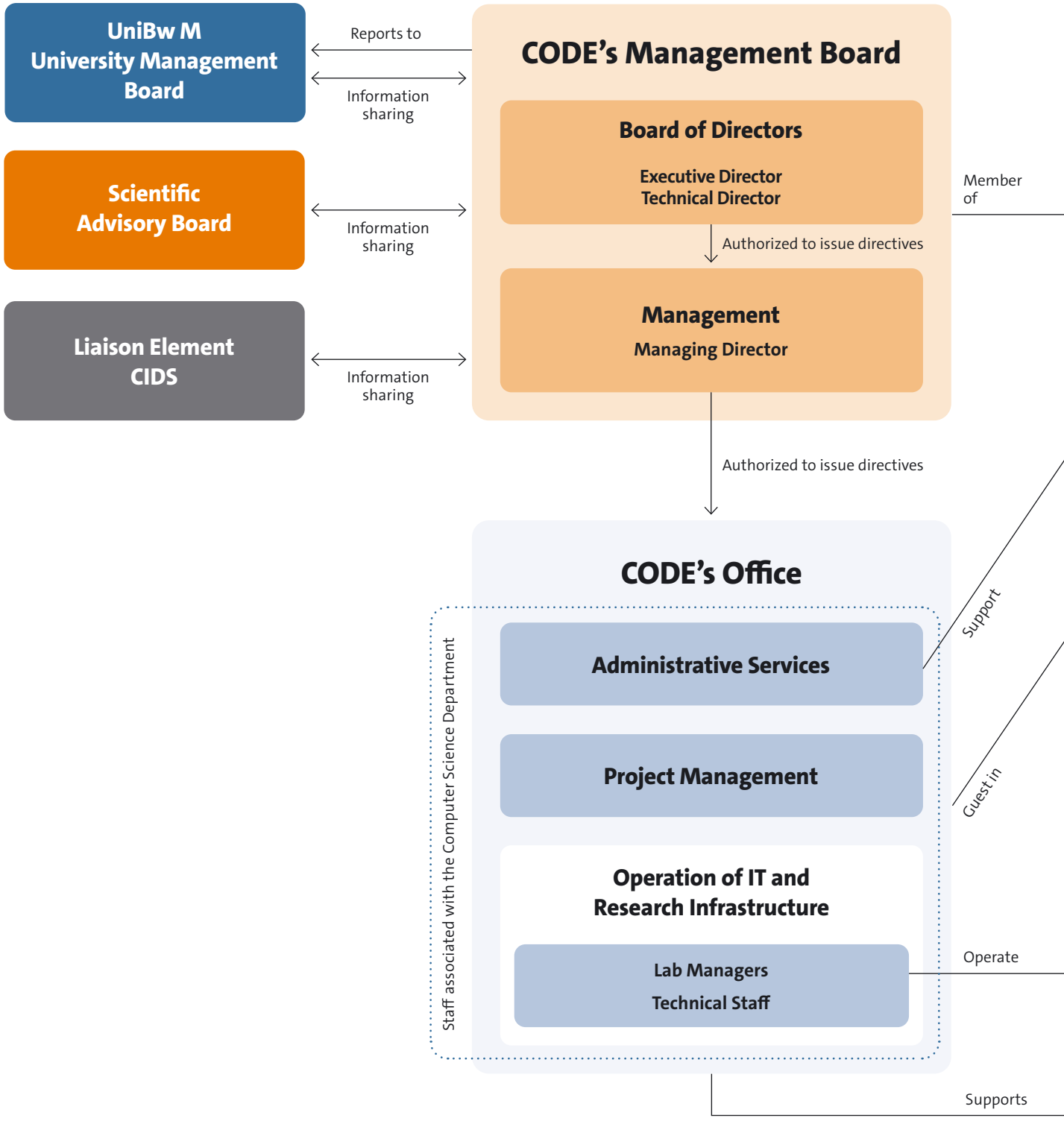
FAIRS, CONFERENCES, SEMINARS

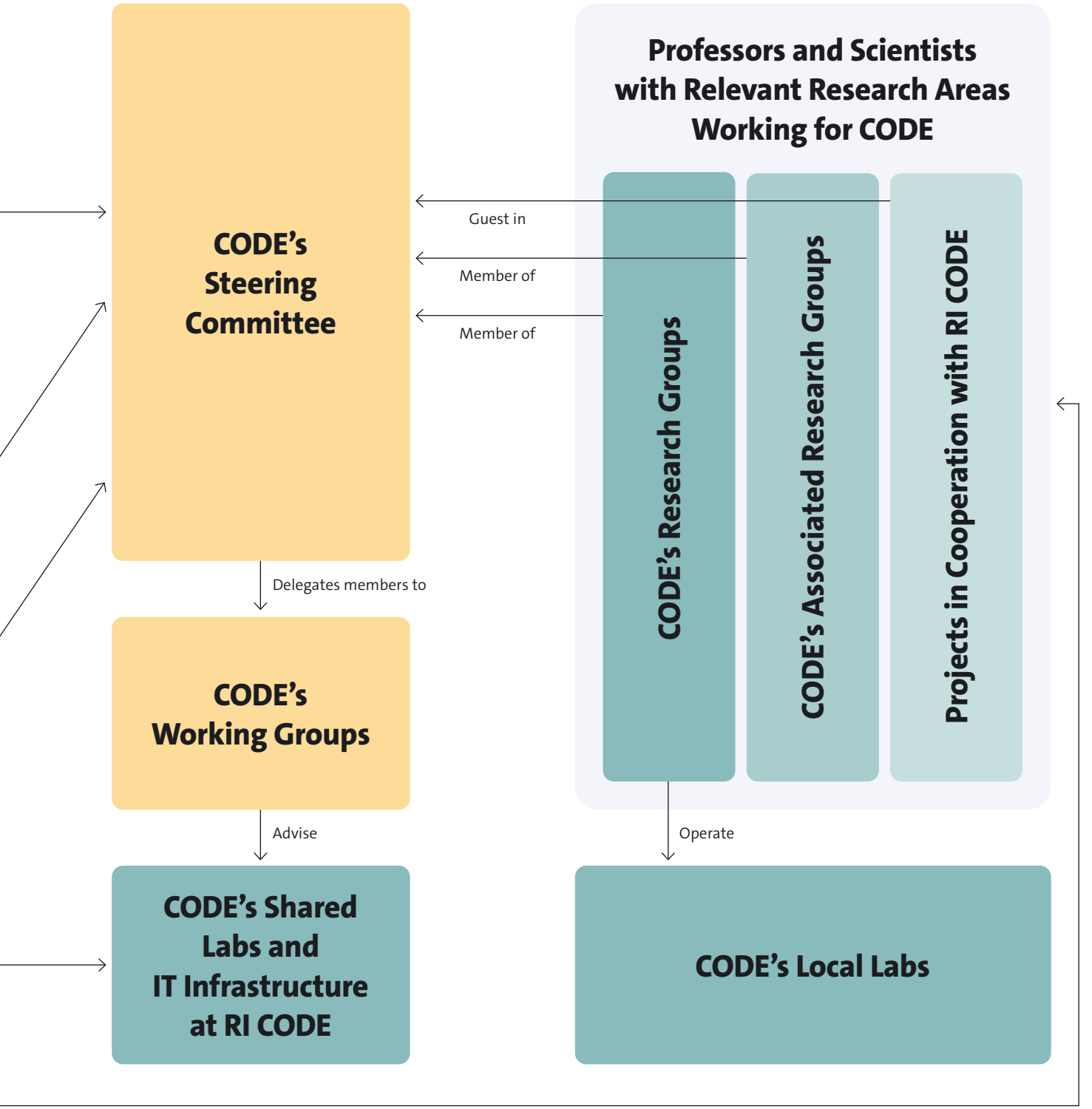
- December 1, 2025 — Online Meeting with Gymnasium Ulricianum Aurich: Professor Wacker presented research of the professorship and CODE and discussed current IT security topics.

ADDITIONAL FUNCTIONS

- Technical and Scientific Director of the UniBw M IT Service Center (RZ)

Organization of RI CODE




CODE's Steering Committee
Professors and Scientists with Relevant Research Areas Working for CODE
CODE's Research Groups
CODE's Associated Research Groups
Projects in Cooperation with RI CODE
Guest in
Member of
Member of
Delegates members to
CODE's Working Groups
Advise
Operate
CODE's Shared Labs and IT Infrastructure at RI CODE
CODE's Local Labs

How to Find Us

Research Institute Cyber Defence and Smart Data (CODE)
University of the Bundeswehr Munich
Carl-Wery-Straße 18
81739 Munich
Germany

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

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

Location Map

Editorial Information

PUBLISHER

Research Institute CODE
University of the Bundeswehr Munich
Carl-Wery-Str. 18
81739 Munich
Germany

MANAGEMENT OF RI CODE

Prof. Dr. Wolfgang Hommel, Executive Director

Prof. Dr. Michaela Geierhos, Technical Director

Marcus Knüpfer M. Sc., Managing Director (until 12/2025)

Stefanie Molnar, M.A., Acting Managing Director (since 01/2026)

PD Dr. Daniela Pöhn, Acting Managing Director (since 01/2026)

PROFESSORS AT RI CODE

Prof. Dr. Harald Baier, Professor for Digital Forensics

Prof. Dr. Stefan Brunthaler, Professor for Secure Software Engineering

Prof. Klaus Buchenrieder, PhD, Professor for Embedded Systems/ Computers in Technical Systems

Prof. Dr. Gabi Dreo Rodosek, Professor for Communication Systems and Network Security

Prof. Dr. Michaela Geierhos, Professor for Data Science

Prof. Dr. Marta Gomez-Barrero, Dean of Studies of the Faculty for Computer Science at UniBw M, Professor for Machine Learning

Prof. Dr. Udo Helmbrecht, Honorary Professor at RI CODE

Prof. Dr. Wolfgang Hommel, Dean of the Faculty for Computer Science at UniBw M, Professor for Software and Data Security

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

Prof. Dr.-Ing. Mark Manulis, Vice Dean of the Faculty for Computer Science at UniBw M, Professor for Privacy

Prof. Dr. Eirini Ntoutsi, Professor for Open Source Intelligence

Prof. Dr. Corinna Schmitt, Adjunct Professor for Secure Communication Systems

Prof. Dr. Daniel Slamanig, Professor for Cryptology

Prof. Dr. Arno Wacker, Professor for Applied Security Analysis (formerly Privacy and Compliance)

All at the Faculty of Computer Science at the University of the Bundeswehr Munich

CODE ASSOCIATED PROFESSORS

Prof. Dr. Ulrike Lechner, Professor for Business Informatics, Faculty of Computer Science

Prof. Dr.-Ing. Carmen Mas Machuca, Professor for Communication Networks, Faculty of Electrical Power Systems and Information Technology

Juniorprof. Dr. Maximilian Moll, Junior Professor for Operations Research – Prescriptive Analytics, Faculty of Computer Science

Prof. Dr.-Ing. Vladislav Nenchev, Professor for Embedded Systems, Faculty of Electrical and Computer Engineering

Prof. Dr. Christoph Peters, Professor for Digital Process Management, Faculty of Business, Economics and Organizational Sciences

Prof. Dr. Stefan Pickl, Professor for Operations Research, Faculty of Computer Science

Prof. Dr. Gunnar Teege, Professor for Distributed Systems, Faculty of Computer Science

All at the University of the Bundeswehr Munich

MEMBERS OF THE ADVISORY BOARD (IN 2025)

From the Faculty for Computer Science at the University of the Bundeswehr Munich

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Ulrike Lechner

Prof. Dr.-Ing. Helmut Mayer

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

OTHER MEMBERS

Wolfgang Sachs, IC II 5, Federal Ministry of Defence

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

Dr. Kai Martius, secunet Security Networks AG

Prof. Dr. Johann Pongratz, TU Dortmund

EDITING AND COORDINATION

Benjamin Bellgrau, M. Sc., Public Relations Officer

Theresa Merkl, Communication Designer

ART DIRECTION

Tausendblauwerk Design Agency, Michael Berwanger

www.tausendblauwerk.de

PRINTED BY

druckhaus köthen

https://koethen.de

REGULATIONS

First Edition, 350 copies

Editorial Deadline: May 2026

Title illustration: Adobe Stock / mankjon

ISBN: 978-3-98997-010-6 | ISSN: 2748-9485

Also published as an electronic publication
(ISBN: 978-3-98997-011-3 | ISSN: 2748-9507)
as well as in German
(ISBN: 978-3-98997-008-3 | ISSN: 2748-8780).

Disclaimer

The figures and information contained in this annual report have been carefully researched and, unless otherwise noted, are current as of December 31, 2025. Despite careful review, no guarantee can be given as to their correctness, completeness, or actuality. Errors and subsequent changes are reserved.


Universität der Bundeswehr München
CODE
RI
Research Institute
Cyber Defence
Universität der Bundeswehr München