Universität der Bundeswehr München

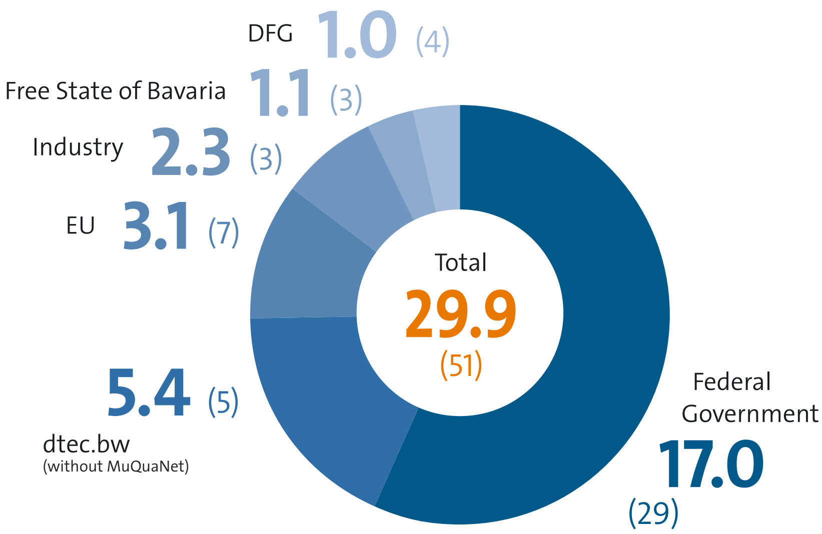
CODE
ANNUAL REPORT
2023

Research Institute Cyber Defence
Universität der Bundeswehr München

Project Funding

In 2023, a total of 51 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

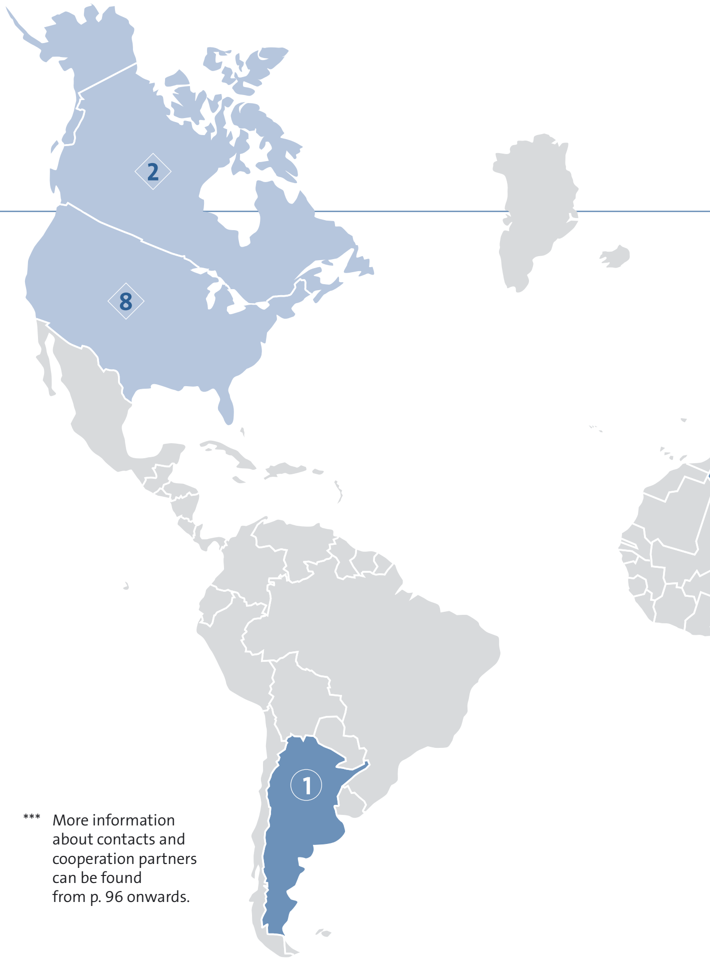
Participating Professorships

Hon.-Prof. Dr. Udo Helmbrecht
Prof. Dr. Michaela Geierhos
Prof. Dr. Florian Alt
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 2023, CODE employees came from 16 countries.

Cooperation Partners***

In 2023, RI CODE cooperated with 130 partners in 35 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. 96 onwards.

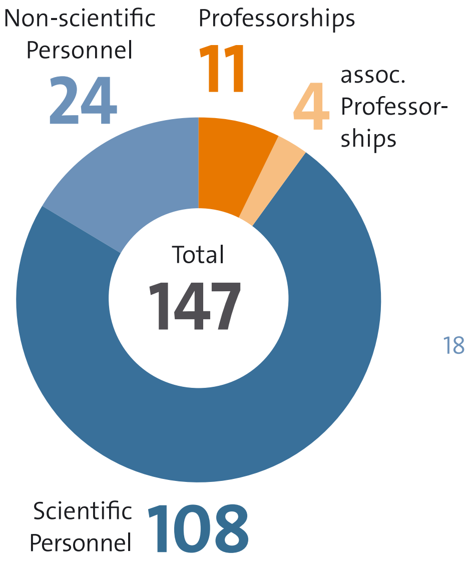
Staff Structure

RI CODE had a total of 147 employees in 2023.
22% percent of staff were women.

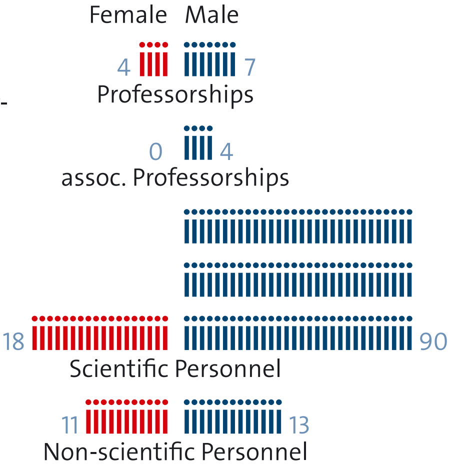
Research Work

Overview of doctorates and
publications at RI CODE 2023

Employees



Gender Share



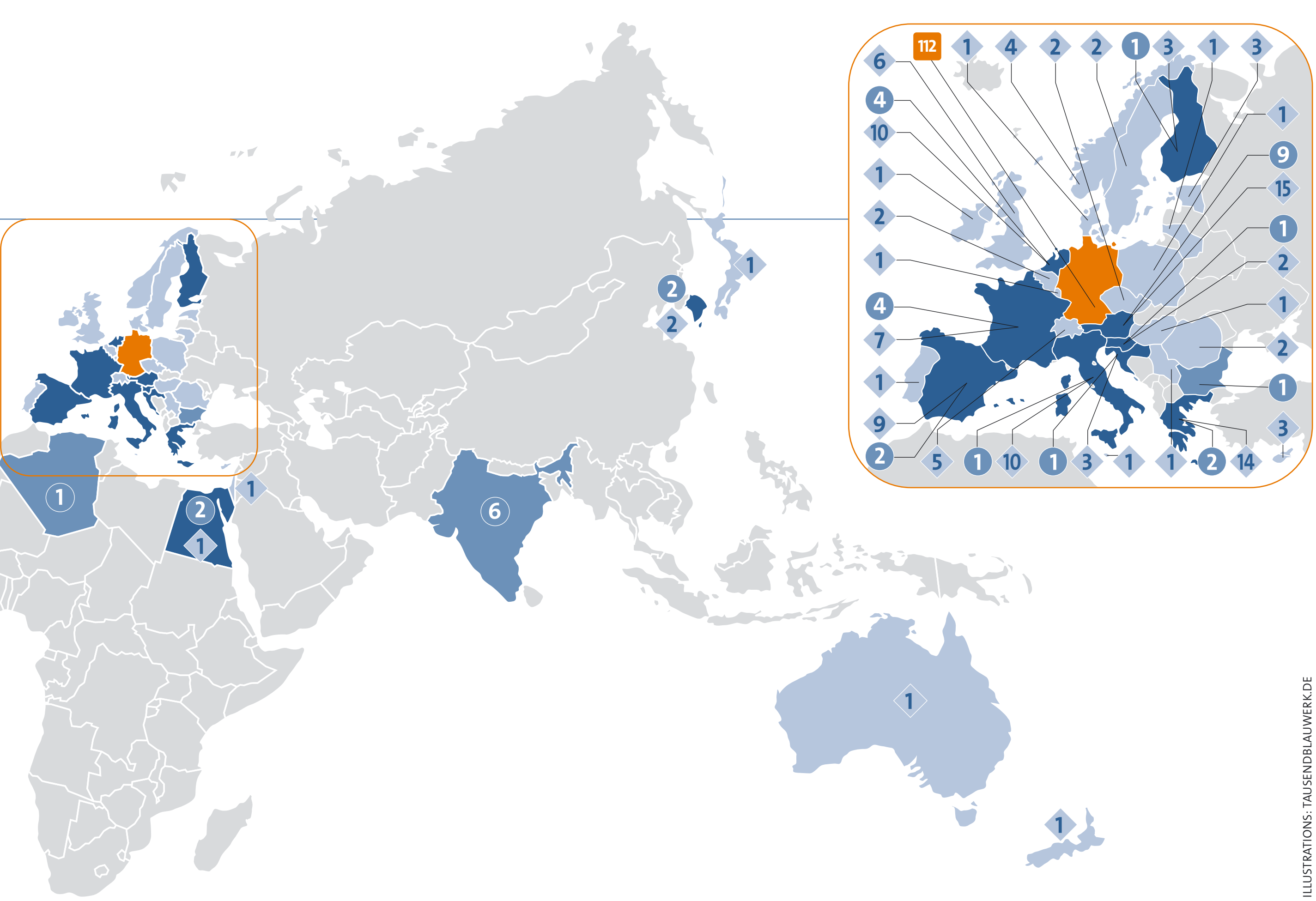
22% 78%

Doctorates

6

Publications

107



ILLUSTRATIONS: TAUSENDBLAUWERK.DE

Universität der Bundeswehr München

CODE
ANNUAL REPORT
2023

Research Institute
Cyber Defence
Universität der Bundeswehr München

Preface by the President

The year 2023 was dominated by the historic anniversary “50 years of the Bundeswehr University Munich”, which we celebrated with numerous events. This was perfectly complemented by the tenth anniversary of CODE.

Since its foundation in 2013, CODE aims to research and develop technical innovations and concepts for the security of data, software and systems in an interdisciplinary approach that is both fundamental and application oriented. To this end, CODE brings together scientific expertise from a wide range of fields and has been working closely with partners from the Bundeswehr, authorities, research and industry for ten years now. CODE therefore fits in perfectly with the motto of the University of the Bundeswehr Munich: “Security and Sustainability in Technology and Society”. In view of the major challenges posed by the “Zeitenwende” (changing times), it is a central concern of mine to establish our university even more as a strategic resource for the Federal Ministry of Defence (BMVg) and the Bundeswehr.

The Research Institute CODE (RI CODE) has been a reliable partner in the German National Coordination Center for Cybersecurity in Industry, Technology and Research (NCC-DE) since 2021. The NCC-DE is a joint cooperation platform of the BMWK, BMI, BMVg and BMBF as well as individual subordinate areas (BSI and RI CODE and DLR-PT). 2023 was an important year for RI CODE in setting the course for further development in the NCC-DE As part of a call for proposals from the European Commission’s Digital Europe Program (DIGITAL), a consortium consisting of BSI, the project management organization at the German Aerospace Center, and RI CODE acquired the project “NCC-DE – Capacity Building for the German National Coordination Centre for Cybersecurity in Industry, Technology and Research”.

In the field of quantum computing, RI CODE is also playing a pioneering role. At the “Quantum Computing Meets Cyber Security” symposium in Garching, which was jointly organized by Munich Quantum Valley, LMU Munich and RI CODE, experts from various fields discussed cybersecurity risks in the age of quantum computers.

We at our university can truly be proud of RI CODE as a success story. I would like to congratulate all those who have contributed to the development and achievements of RI CODE over the past ten years and wish them all the best for the future and continued success! With this in mind, I hope you enjoy reading this special annual report!

With best regards,

Kern

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

Dear Readers,

Wolfgang Hommel, Marcus Knüpfer, Michaela Geierhos

For us, 2023 was also characterized by the joint anniversary of 50 years of the University of the Bundeswehr Munich and ten years of CODE. Part of our annual conference was also dedicated to this anniversary – including a birthday cake. However, much has also developed at the Research Institute CODE. In a familiar style, this annual report gives you an insight to selected highlights, the exciting work of our research groups and the broad spectrum of our activities over the past year.

We are happy to report further growth of RI CODE in 2023. Professor Dr. Marta Gomez-Barrero joined FI CODE in October and Professor Dr. Daniel Slamanig in November, taking over the professorships for Machine Learning and Cryptology, respectively. Due to the growth of our existing research groups, the number of CODE employees rose to over 140. For the first time, our research groups worked on over 50 third-party funded projects in parallel. A selection of these research projects is presented in more detail in the main section of this annual report.

Successful research also includes the transfer into practice, which we foster through close networking with experts from the Bundeswehr, authorities and industry.

In 2023, we organized numerous events with selected cooperation partners and hand-picked participants that were profitable in terms of content and promoted cooperation. The topics covered ranged from the intersection between quantum computers and cyber security to open source intelligence. A brief summary of these events can also be found in this report.

As a university-based institution, we are particularly happy about the increasing importance of continuous professional and personal education. With the expansion of our Cyber Range and the hands-on training courses held there for the Bundeswehr and state criminal police offices, the lead role in the further development of the internationally popular e-learning platform CrypTool by Professor Dr. Arno Wacker's research group and the participation of about 60 teams in our Capture the Flag event, CODE is making a professionally focused and high-quality contribution to the subject of lifelong learning.

We hope you enjoy reading our 2023 Annual Report and gain interesting insights and new knowledge, and we are looking forward to continuing the successful collaboration with you!

Wolfgang Hommel

Prof. Dr. Wolfgang Hommel

Michaela Geierhos

Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Management of the Research Institute CODE

FIG.: UNIBW M; A. WAGENER FOTOGRAFIE

Contents

ABB.: ADOBE STOCK / KILLYKOON

CONTENTS

Highlights
From the Institute

12 Happy Birthday, CODE!
18 Report on the CODE Annual Conference 2023
22 Report on the CRITIS Conference 2023
26 “Cyber Phoenix” Reserve Exercise
28 Quantum Technologies
34 Quantum Computing Meets Cyber Security
35 First Cyber Awareness Training Hosted by JSEC
36 CrypTool Symposium 2023
37 OSINT Forum 2023
38 Bundeswehr’s Head of CIT Department Visits CODE
39 Excellence Award for Stefan Pickl

Research
Portraits and Projects

42 Research at RI CODE

44 Usable Security and Privacy:
Prof. Dr. Florian Alt
- Project PriMR
- Project User-Centered Biometric Interfaces

48 Digital Forensics:
Prof. Dr. Harald Baier
- Investigation of Do-It-Yourself Drones
- Illegal WhatsApp stickers on Android

52 Secure Software Engineering:
Prof. Dr. Stefan Brunthaler
- Looming Danger of Supply-Chain Attacks
- Binary Component Identification

56 Data Science:
Prof. Dr. Michaela Geierhos
- Project SynData
- Project NAWI

60 Software and Data Security:
Prof. Dr. Wolfgang Hommel
- Project ACSE
- Project LIONS

64 PACY:
Privacy and Applied Cryptography Lab:
Prof. Dr.-Ing. Mark Manulis
- Asynchronous Remote Key Generation
- Fast and Expressive Searchable Encryption

68 Open Source Intelligence:
Prof. Dr. Eirini Ntoutsi
- Project NoBIAS
- Project STELAR

72 Cryptology:
Prof. Dr. Daniel Slamanig
- Fine-Grained Forward Security via Puncturable Encryption
- Strengthening Non-Interactive Zero-Knowledge Proofs

76 Privacy and Compliance:
Prof. Dr. Arno Wacker
- The CrypTool Project
- Detection of Cookie Banners

Further Projects

80 Communication Systems and Network Security:
Prof. Dr. Gabi Dreo Rodosek

82 BioML: Biometrics and Machine Learning Lab:
Prof. Dr. Marta Gomez-Barrero

84 Quantum Communication:
Prof. Dr. Udo Helmbrecht

86 Operations Research - Prescriptive Analytics:
Junior Prof. Dr. Maximilian Moll

88 Operations Research - Research Group COMTESSA:
Prof. Dr. Stefan Pickl

90 National Coordination Center for Cybersecurity:
PD Dr. Corinna Schmitt

92 Formal Methods for Securing Things (FOMSET):
Prof. Dr. Gunnar Teege

Cooperations
Germany and the World

96 National Partners
100 Internationality

Young Science
Offers and Opportunities

104 Study Award 2023
108 Doctorates 2023
110 Capture the Flag 2023

Addendum
Publications and Activities

114 Usable Security and Privacy
116 Digital Forensics
117 Secure Software Engineering
118 Data Science
119 BioML: Biometrics and Machine Learning Lab
120 Quantum Communication
120 Software and Data Security
122 Privacy and Applied Cryptography Lab
123 Operations Research – Prescriptive Analytics
124 Open Source Intelligence
125 Operations Research – Research Group COMTESSA
126 Cryptology
127 Formal Methods for Securing Things (FOMSET)
127 Privacy and Compliance

Organizational Structure

128 Organization of RI CODE

Categories

2 Facts and Figures
8 Our Mission Statement
130 Contact Information
131 Editorial Information

OUR MISSION STATEMENT

FIG.: ADOBE STOCK / STNAZKUL

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 defence, 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) organizational unit, 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 / ALI

Highlights

From the Institute

Happy birthday, CODE!

Milestones in our development in the first ten years

CODE's anniversary is a good opportunity to look back on the past ten years. In this article, we summarize the history of CODE's origins as an in-house university research center, its growth to become a departmental research institute, and other milestones on the way to its current range of services. Special thanks go to our forerunners from both the University and the Bundeswehr, as well as our long-time cooperation partners.

SINCE THE PRESIDENCY (2005 - 2022) of Prof. Dr. Merith Niehuss, the guiding principle of "Security and Sustainability in Technology and Society" has shaped research at the University of the Bundeswehr Munich (UniBw M). The aim of building a scientific profile with social responsibility is also achieved to a large extent through the university's internal research centers. After approval by the Senate and the university management, CODE was founded in 2013 as the fourth research center on the initiative of Prof. Dr. Gabi Dreo Rodosek, the spokeswoman of the Research Center CODE and first Executive Director of the later Research Institute CODE (RI CODE), and the former Dean of the Faculty of Computer Science, Prof. Dr.-Ing. Mark Minas.

The kick-off event of the still young Research Center CODE took place in September 2013 under the premise of pooling and coordinating research in the field of cyber defence both within the university and with external cooperation partners and also transferring research results into practice. In the following years, this event developed further to become the CODE Annual Conference, an event that fills the university's main auditorium every year and, since 2018, also includes the Cyber/IT Innovation Conference of the Federal Ministry of Defence (BMVg). One of the many prominent speakers at the first event was Dr. Thomas Daum, UniBw M alumnus in computer science and now Inspector of the Cyber and Information Domain Space (CIDS).

Kick-off event of the Research Center CODE in September 2013.

FIG.: RI CODE / A. WAGENER; RI CODE

Opening of the UniBw M Cyber Cluster at the CODE Annual Conference 2017 by Federal Minister of Defence Dr. Ursula von der Leyen.

With cyber defence as a strategic field of research and activities at the university, the Faculty of Computer Science dedicated a first new full professorship to the IT security of software and data in 2014, to which Prof. Dr. Wolfgang Hommel was appointed in 2016.

As part of the plans to establish the CIDS as an independent military organizational unit of the Bundeswehr, the expansion of CODE into a departmental research facility was planned under the leadership of Armin Fleischmann and Bernd Schlömer at the Federal Ministry of Defence. Under Prof. Klaus Buchenrieder, Ph.D. (then Dean of the Faculty of Computer Science and subsequently the first Technical Director of FI CODE) and the former Chair of the Senate, Prof. Dr.-Ing. habil. Dr. mont. Eva-Maria Kern, MBA, CODE received a charter as a research institute with fundamental personnel and material resources.

The advancement of CODE to a research institute was accompanied by the launch of the Master's degree program in Cyber Security. The UniBw M Cyber Cluster, which is unique in Germany, was officially opened by the Federal Minister of Defence, Dr. Ursula von der Leyen, at the CODE Annual Conference 2017.

Close collaboration with ZITiS

In addition to eleven new W3 professorships, RI CODE also established an office, which was headed by Managing Director Volker Eiseler. In order to meet the additional demand for office and lab space among the new research groups, the planning of a new building on the university campus began in 2016. In 2017, the institute then moved to rented office space in "Cascada", an office building in the south of Munich close to the UniBw M campus. This also became home to the staff of the Central Office for Information Technology in the Secu-

Home of RI CODE since 2017: The "Cascada" office building in the southeast of Munich.

Vice Admiral Dr. Thomas Daum, Inspector CIDS, (4th from left) visits the Cyber Range at RI CODE in 2021.

rity Sector (ZITiS), which was also established in 2017. The close cooperation between RI CODE and ZITiS from the very beginning was not only apparent in the fact that the planned new building on the university campus was to be used by both organizations, but also in research and teaching. For example, the Master's degree program in Cyber Security was one of the first courses at UniBw M with a dedicated capacity for non-military students. A substantial number of these students have been dispatched by ZITiS. For these students, a specialized track with a tailor-made graduate profile was therefore introduced in 2020.

Transferring research results into practice

In light of the personnel requirements in the command, organizational area and CIDS, the further development of research and teaching at RI CODE is also closely monitored and supported. Among the frequent guests of the research institute were and are Ludwig Leinhos, first Inspector CIDS, Jürgen Setzer, Deputy Inspector CIDS, and Michael Vetter, Head of Department CIT I at the BMVg. To ensure a forward-looking research orientation and organizational development, an advisory board was established, which includes Wolfgang Sachs, Head of Division CIT I 2, as well as representatives from industry and science. A liaison element was installed on the initiative of Armin Fleischmann to ensure a close exchange and stimulate the transfer of research results into the practical application for the troops. The liaison officers also have the exclusive opportunity to participate directly in research projects and thus gain further scientific qualifications.

Further growth and new fields of research

As the research center became a research institute, the topics of Artificial Intelligence and machine learning applications – referred to under the term "Smart Data" – became CODE's second major field of research. Prof. Dr. Michaela Geierhos was appointed to the Data Science professorship, the first professorship in this new CODE business area, in 2020. That same year, CODE exceeded 100 employees for the first time and Prof. Dr. Udo Helmbrecht, former President of the Federal Office for Information Technology (BSI) and the European Union Agency for Cybersecurity (ENISA), succeeded Prof. Klaus Buchenrieder, Ph.D., as Technical Director.

Together with Prof. Dr. Gabi Dreo Rodosek, he paved the way for the establishment of CODE's third research field, Quantum Technology. In addition to quantum computing, this also includes secure communication through quantum key distribution and post-quantum

FIG.: RI CODE(2); UNIBW M / SIEBOLD

Visit by the Inspector General of the Bundeswehr, General Eberhard Zorn in 2022.

cryptography. After retiring at the beginning of 2021, Prof. Dr. Wolfgang Hommel succeeded him as Technical Director. In the midst of the COVID-19 pandemic – the CODE Annual Conference was held as a virtual event in 2020 and 2021 – the establishment of the new research field Quantum Technology began under the direction of Dr. Sabine Tornow. First steps were also taken towards RI CODE's participation in the National Cybersecurity Coordination Center (NCC-DE), which is managed by Priv.-Doz. Dr. Corinna Schmitt.

Personnel changes and developments

Significant personnel and organizational changes followed at the end of 2021. Prof. Dr. Wolfgang Hommel became the Executive Director, Prof. Dr. Michaela Geierhos the Technical Director. Marcus Knüpfer succeeded Volker Eiseler as Managing Director, who in turn succeeded Bernd Schlömer in the BMVg.

The sustained expansion of the research institute – 15 research groups were already working at the institute in 2022 – was accommodated with the establishment of an internal steering committee at CODE. In addition to a significantly broader research spectrum and the further development of the Master's degree program in Cyber Security, the years 2022 and 2023 were characterized by offering former internal services to the Bundeswehr and cooperation partners. CODE's Cyber Range is now used by the Bundeswehr, cyber reservists and also state criminal investigation offices. Support is provided to various Bundeswehr branches interested in analyzing the practical potential of and experimenting with quantum computers.

The success story continues

By the end of our anniversary year 2023, CODE now has more than 140 employees working in parallel on over 50 third-party funded projects. We are well established as a departmental research institute and are closely connected with numerous partners in Germany and abroad. We would like to thank all our supporters and look forward to the future together! ■

More information on RI CODE

https://www.unibw.de/code

@ code@unibw.de

FIG.: UNIBW M / SIEBOLD

Overview

Management of Research Institute CODE

Executive Directors

Prof. Dr. Wolfgang Hommel	since 2021
Prof. Dr. Gabi Dreo Rodosek	2017-2021

Technical Directors

Prof. Dr. Michaela Geierhos	since 2021
Prof. Dr. Wolfgang Hommel	2021
Hon.-Prof. Dr. Udo Helmbrecht	2020-2021
Prof. Klaus Buchenrieder, Ph.D.	2017-2020

Managing Directors

Marcus Knüpfer	since 2022
Volker Eiseler	2017-2021

Members of the CODE Advisory Board

Prof. Klaus Buchenrieder, Ph.D.	UniBw M
Dr. Norbert Gaus	Siemens
Prof. Dr. Ulrike Lechner	UniBw M
Prof. Dr.-Ing. Helmut Mayer	UniBw M
Prof. Dr. Johann Pongratz	TU Dortmund
Prof. Dr. Oliver Rose	UniBw M
Wolfgang Sachs	BMVg CIT I 2
Prof. Dr. Gunnar Teege	UniBw M
Dr. Ralf Wintergerst	BITKOM

Master's Degree Program in Cyber Security (MCYB)

Chairmen of the Examination Board

Prof. Dr. Harald Baier	since 2022
Prof. Dr.-Ing. Mark Minas	2021
Prof. Dr. Stefan Brunthaler	2018-2021

Study Program Coordinators

Michael Sattelmayer	since 2020
Stefanie Molnar	2018-2020

Members of the Academic Affairs Committee MCYB

Prof. Dr. Harald Baier, Prof. Dr. Michaela Geierhos, Prof. Dr. Peter Hertling (Dean of Students), Prof. Dr. Wolfgang Hommel, Prof. Dr.-Ing. Mark Manulis, Stefanie Molnar, Prof. Dr. Eirini Ntoutsi, Michael Sattelmayer, Prof. Dr. Gunnar Teege as well as representatives of academic assistants and students

Professorships and Research Groups at RI CODE

Prof. Dr. Florian Alt *Usable Security and Privacy*	since 05/2018
Prof. Dr. Harald Baier *Digital Forensics*	since 09/2020
Prof. Dr. Stefan Brunthaler *Secure Software Engineering*	since 10/2017
Prof. Klaus Buchenrieder, Ph.D. *Embedded Systems / Computers in Technical Systems*	
Prof. Dr. Gabi Dreo Rodosek *Communication Systems and Network Security*	
Prof. Dr. Michaela Geierhos *Data Science*	since 04/2020
Prof. Dr. Marta Gomez-Barrero *Biometrics and Machine Learning Lab*	since 10/2023
Hon.-Prof. Dr. Udo Helmbrecht *Quantum Communication*	
Prof. Dr. Wolfgang Hommel *Software and Data Security*	
Prof. Dr. Ulrike Lechner *Wirtschaftsinformatik*	
Prof. Dr.-Ing. Mark Manulis *PACY:* *Privacy and Applied Cryptography Lab*	since 03/2022
Prof. Dr.-Ing. Helmut Mayer *Visual Computing*	
Prof. Dr. Maximilian Moll *Operations Research – Prescriptive Analytics*	
Prof. Dr. Eirini Ntoutsi *Open Source Intelligence*	since 08/2022
Prof. Dr. Stefan Pickl *Operations Research*	
Priv.-Doz. Dr. Corinna Schmitt *Secure Communication Systems*	
Prof. Dr. Daniel Slamanig *Cryptology*	since 11/2023
Prof. Dr. Gunnar Teege *Distributed Systems*	
Prof. Dr. Arno Wacker *Privacy and Compliance*	since 06/2018

Report on the CODE Annual Conference 2023

CODE celebrates its ten-year anniversary

Ten years of CODE – ten years of cutting-edge research in the fields of Cyber Security, Smart Data and Quantum Technologies. The Annual Conference of the Research Institute CODE on July 11 and 12, 2023 was dedicated to this special anniversary. More than 400 participants from the military, industry, science, and authorities met on the campus of the University of the Bundeswehr Munich.

THE FIRST DAY of the event started with a welcome speech by the President of the Bundeswehr University Munich, Prof. Dr. Eva-Maria Kern, and State Secretary Siemtje Möller, who sent her greetings via video message from the Federal Ministry of Defence. In accordance with the conference motto "10 years of CODE", the Executive Director of RI CODE, Prof. Dr. Wolfgang Hommel, gave a review of the past decade in his speech. During his entertaining journey through the last ten years, he not only gave the audience an insight into the history and development of CODE, but also told one or two amusing anecdotes from this period. Vice Admiral Dr. Thomas Daum then took to the lectern. Among other things, the Inspector of Cyber and Information Domain Service referred to the capabilities of Artificial Intelligence. He demonstrated this with an impressive example: The introduction to his keynote was written entirely by ChatGPT, as the Vice Admiral explained in the course of his speech.

Barbara Kluge from the Federal Ministry of the Interior and Community (BMI) spoke about the fact that cybersecurity research in particular can only succeed by working together. She particularly emphasized the close cooperation between the BMI and RI CODE on this topic. During the intermissions "At Ease", the university's big band, entertained the audience with lively musical interludes. In doing so, they performed

Vice Admiral Dr. Thomas Daum, Inspector of Cyber and Information Domain Service: "At CODE, the technology of the future becomes the technology of today."

From left to right: Marcus Knüpfer (Managing Director RI CODE), Michael Dreher (IBM), Prof. Dr. Michaela Geierhos (Technical Director RI CODE), David Faller (IBM), Prof. Dr. Wolfgang Hommel (Executive Director RI CODE) and Prof. Dr. Geralt Siebert (Vice President UniBw M).

ALL FIG.: UNIBW M / SIEBOLD

film music classics such as “Happy” and “Golden Eye”. After a short coffee break, the program continued with presentations by State Secretary Bernd Schlömer and ZITiS President Wilfried Karl. Schlömer spoke about the prospects for the federal state of Saxony-Anhalt in terms of digitalization and information security in cross-level cooperation between the state and local authorities. Wilfried Karl also picked up on the aspect of cooperation, thereby calling cooperation and knowledge “the foundation of cyber security”. Right before the lunch break, another highlight followed. IBM and UniBw M extended their partnership in the field of quantum computing for a further five years. The contract was signed by representatives from both sides in a festive ceremony. As a Quantum Innovation Center, this opens up further opportunities for research and teaching in this promising field, particularly for RI CODE.

State Minister Dr. Herrmann praises work of CODE

Further presentations followed after the lunch break, including those by Prof. Dr. Harald Baier and Prof. Dr. Eirini Ntoutsi, who gave insights into current research at RI CODE in their contributions on Digital Forensics and Responsible AI, respectively. The last event block of the afternoon focused on the topic of “Software-defined Defence”. In his introductory presentation, Michael Kiefer from Dassault Systems Germany explained the importance and topicality of the subject once again. Jens Ohlig from the daily paper *Tagesspiegel Background* then discussed the topic in a panel discussion together with representatives from the military, industry and interest groups. At the end of the first day of the event, the social event took place in the UniCasino, where the Bavarian State Minister for Federal and Media Affairs, Dr. Florian Herrmann, gave a dinner speech. “The Research Institute CODE is a flagship of the Bundeswehr in Bavaria. Since 2013, CODE has been the perfect example of how good, networked cooperation in the field of cyber security works,” said the Minister of State. He emphasized: “Defence is always a team task. We will continue to rely on close cooperation with CODE, whose excellent research work makes a decisive contribution to security in the digital space.”

After the welcome address by the Technical Director of FI CODE, Prof. Dr. Michaela Geierhos, day two of the CODE Annual Conference began with two keynotes. Brigadier General Armin Fleischmann, Head of Cyber/

In light of the increasing importance of cybersecurity issues, State Minister Dr. Florian Herrmann particularly highlighted the work of RI CODE in his dinner speech.

The winner of the Cyber/IT Innovation Conference was Dr. Michael Kissner (m.). Brigadier General Armin Fleischmann (l.) and Prof. Dr. Wolfgang Hommel (r.) congratulated him on his success.

Information Technology I at the BMVg, once again picked up on the topic of software-defined defence and spoke about the advantages and challenges of a stronger focus on software in capability development. In a second keynote, Prof. Dr. Achim Walter from the University of Kiel emphasized the importance of attention and active framework conditions in order to promote innovation in the best possible way and "bring it to life". His inspiring talk was a perfect thematic introduction to the innovation conference in the afternoon. The rest of the morning offered the opportunity for in-depth discussions and presentations: In the five workshops held in parallel, participants explored topics including cyber range training in the context of critical infrastructures, the challenges and opportunities of Artificial Intelligence, and quantum technologies.

Cyber/IT Innovation Conference

At the Cyber and Information Technology Innovation Conference, which was organized in cooperation with the BMVg, innovative ideas that could potentially be used in the BMVg's business area were presented in the afternoon. This year's first prize of 15,000 euros went to Dr. Michael Kissner from Akhetonics GmbH, who impressed the jury and the audience with an optical, universal high-performance processor for homomorphically encrypted data. However, the other presentations on the day also highlighted the potential applications for innovations in the Bundeswehr. In his opening remarks, Brigadier General Fleischmann made it clear: "All of today's presentations are already winners."

The annual conference ended with a summary and closing remarks by Prof. Dr. Michaela Geierhos. She thanked all participants for their attendance, especially those who had contributed to the anniversary conference in various ways - whether on or off stage. ■

More information on the CODE Annual Conference

🌐 www.unibw.de/code/events/jahrestagungen

🌐 www.youtube.com/c/FzcodeDeubw

@ code@unibw.de

FIG.: UNIBW M / PLANK; RI CODE / B. BELLGRAU

Report on the CRITIS Conference 2023

The new reality of safety & security

CRITIS 2023 was the 18th International Conference on Critical Information Infrastructures Security, held from September 13 to 15, 2023 at Laurea University in the Helsinki metropolitan region in Finland. After the first successful cooperation in Munich in 2022, CRITIS 2023 was organized again in scientific cooperation with CODE, with Prof. Dr. Udo Helmbrecht as Honorary Chair and Prof. Dr. Stefan Pickl as Program Co-Chair.

THE AIM OF the conference CRITIS 2023 was again to bring together researchers, academic professionals, critical information infrastructure operators, industry and governmental organizations working in the field of complex infrastructure system security, and especially in operations research. In this current context, CRITIS 2023 was primarily, but not exclusively, concerned with research topics that address the security of information exchange and securing information infrastructures in various ways, while also promoting topics related to hybrid threats and optimizing the security of critical information infrastructures.

Safety & security and operations research

Additionally, CRITIS 2023 aimed to nurture and inspire young and open-minded researchers in this challenging multidisciplinary research field of safety and security, especially in connection with operational analysis. The CRITIS 2023 conference continued the tradition of bringing forth innovative research in the field of critical information infrastructures protection C(I)IP, exploring ideas that address challenges to resilience and societal safety and security, and fostering dialogue with stakeholders. The opening of the conference was given by the General Chair and Director of LAURA Security Research Program, Päivi Mattila.

The new reality of security

Prof. Dr. Bernhard M. Hämmerli, former president of the Information Security Society Switzerland ISSS, welcomed the colleagues and addressed special thanks from the steering committee to the organizers. He was also thankful that Prof. Dr. Udo Helmbrecht from CODE acted again as Honorary Chair of CRITIS 2023. He also thanked CODE for the excellent scientific cooperation.

Afterwards, RDI Vice President Mari Vuolteenaho officially opened the conference and introduced the first keynote speaker, Prof. Dr. Jarno Limnéll from the Finnish Parliament. The title of his inspiring talk was “The new reality of security”.

CRITIS
2023
SEPTEMBER 13-15
The Interna... Conference on
Critical In... Infrastructures
Security ...ki metropolitan
region i...
KEAKOULU
...ed Sciences

Prof. Dr. Stefan Pickl with the local organizer Päivi Mattila and the plenary speaker Prof. Dr. Kenji Watanabe (f. l. t. r.).

FIG.: ADOBE STOCK / V. GALKINA; RI CODE / S. PICKL

Plenary talk on cyber-physical security in CIs

Also Peter Sund, CEO of the Finnish Information Security Cluster (FISC), Technology Industries of Finland, addressed future challenges of safety and security, as well as the analytic needs and relevance of suitable models.

After the coffee break, Kenji Watanabe (Nagoya Institute of Technology) presented the first plenary speech about “Challenges for operational implementation of the cyber-physical security in CIs”. He stressed the importance of suitable models, algorithmic approaches, and also efficient data-driven optimization techniques and OR-based approaches in the special context of critical infrastructures.

Intelligent decision support tools – hybrid threats

The next session was opened by the contribution “Towards an ecosystemic analysis for essential and important entities” presented by Nicolas Mayer. A “Decision support system for the monitoring and risk analysis of national critical entities” was developed and characterized by Roberto Setola. Findings from the interesting MEDEA project were discussed by Genny Dimitrakopoulou in the talk “Hybrid cyber attacks on critical infrastructure”.

The other parallel session focused on risk management and risk analysis: Hiroshi Sasaki demonstrated how he had developed an easy risk assessment tool for factory cybersecurity. José Martí analyzed a climate change risk framework in relation to a complex interdependent critical systems/ complex interdependent critical system.

Energy security and prediction of maritime traffic

“Assessing the effect of the lack of essential workforce on the economic sectors during a pandemic” was presented by Roberto Setola. The role of a complex spectrum analysis was discussed in the talk “Evasion attack against multivariate singular spectrum analysis-based IDS” given by Vikas Maurya.

After the coffee break, energy security was in the focus of the conference: The first plenary speech was given by Vytis Kopustinskas (Joint Research Centre of Europe) about “Lessons learned from tabletop exercises: Coherent resilience of energy supply in the Baltic states”. The second plenary speech was presented by Jukka Heikkonen (University of Turku) about “AI for anomaly detection with examples in maritime”. Both plenary sessions were discussed in depth during the subsequent lunch break. After the lunch break, the following contributions were treated in parallel sessions: “Surveillance of offshore installations with patrol routine” by Bartosz Skobiej, “Vulnerability analysis of an electric vehicle charging ecosystem” by Roland Plaka, and “GNSS signal monitoring and security of supply of GNSS-based services” was presented by Mika Saajasto.

SEPTEMBER 13–15
CRITIS 2023
The International Conference on Critical Information Infrastructures Security In the Helsinki metropolitan region in Finland

Plenary lecture by Major General (ret.) Dr. Dr. Dieter Budde.

SANCTUM+

Les promesses de SANCTUM+

L'HUMAIN…

Marier « sciences douces » et « sciences dures »

L'efficacité de la modélisation repose sur la connaissance et la description aussi fidèle que possible des « fonctionnements » humains auxquels elle entend se substituer.

L'apport des sciences humaines et sociales est donc fondamental, de même que des travaux comme ceux sur techniques cognitives, ou les heuristiques, qui s'efforcent de décrypter les mécanismes implicites l'activité humaine.

ET LA MACHINE.

Un recours intensif à l'intelligence artificielle

L'automatisation de la production des « uchronies » recherchée par SANCTUM+ a pu longtemps apparaître comme chimérique.

Il en fut d'ailleurs ainsi en météorologie, dans les débuts de la prévision numérique, il y a près d'un demi-siècle. Aujourd'hui, avec des prévisions supérieures à 10 jours et d'un haut niveau de fiabilité, les supercalculateurs sont capables de prévoir le temps bien au-delà des capacités humaines.

La comparaison – à une époque plus récente – peut être étendue aux jeux de stratégie comme les Échecs et le Go. la capacité d'anticipation y est déterminante. Réputée propre au genre humain, cette capacité cognitive a finalement été dépassée par des modélisations informatiques.

Le jeu de Go correspond de près à la méthodologie SANCTUM+. Chaque joueur déploie ses pions comme autant d'actifs destinés à acquérir le meilleur contrôle possible du [illegible]. L'importance du nombre de possibilités – bien supérieures à celles du jeu d'Échecs – a [illegible] l'ordinateur durablement en infériorité par rapport à l'homme. **L'utilisation des réseaux de neurones et le recours au « deep learning » sont finalement venus à bout de la suprématie humaine.**

Nouvelles technologies

Si les capacités informatiques en vitesse de traitement et de stockage semblent respecter la loi de Moore (1965) et offrir par cycle de temps des capacités inégalées, le réel fait nouveau est **l'apparition du Big Data et la multiplication des objets connectés.**

SANCTUM+ peut ainsi raisonnablement faire l'hypothèse d'une initialisation la plus fine et la plus rapide possible de ses modèles et d'assumer leur complexité croissante.

L'architecture Von Neumann qui a permis de résoudre [illegible]

[illegible]

Nouveaux modèles

C'est la révolution conceptuelle introduite par la **« prévision d'ensemble »** qui a permis à la météorologie moderne d'effectuer des prévisions à moyenne échéance d'un haut niveau de fiabilité. Son principe qui consiste à partir d'un échantillon des états initiaux pour aboutir à un échantillon des états prévus n'est plus spécifique à la météorologie. Il est donc transposable à un système comme SANCTUM+.

"En s'efforçant de prévoir l'issue de la bataille, ou risque de l'erreur, le stratège accroît sa force face à l'adversaire."
CARL VON CLAUSEWITZ

SDSIE Le SDSIE est le service du haut fonctionnaire de défense et de sécurité des MTES/MCTRCT
Secrétariat général · 92055 La Défense CEDEX · Tél : +33 (0) 1 40 81 21 22 · www.ecologique-solidaire.gouv.fr · www.cohesion-territoires.gouv.fr
Contact : sanctum@developpement-durable.gouv.fr · www.projet-sanctum.com

SANCTUM+
SYSTÈME D'ANTICIPATION DE CRISE PAR TRAITEMENT UCHRONIQUE MODÉLISABLE

PROJET D'AIDE À LA PRISE DE DÉCISION STRATÉGIQUE

Strategic decision support in the context of the international SANCTUM+ research network.

The stream was opened by the talk "Relationships between security management and technical security" by Øyvind Toftegaard. "Business continuity building dynamic resilience" was discussed from different perspectives by Eveliina Hytönen. David Prette gave an overview on "Emergency resilience closer to citizens' understanding".

The final session was opened by two very interesting plenary talks. Christian Després, Ministry of Ecological Transition, France, focused on anticipation concepts in the context of "Anticipating future crises situations and adapting the means to respond to them". He referred to the special cooperation and research activities between the research group COMTESSA and SANCTUM Labo-Crise. Mr. Evaldas Bružė from the Lithuanian Cyber Crime Center of Excellence for Training, Research & Education, stressed the consideration of human behavior in analytic models. Two industry presentations associated the connection cyber security and operational analysis: Mikaeli Langinvainio, CEO of Inclus Ltd., highlighted artificial intelligence and enhanced risk management. The last talk characterized the Cyber Security Index and the need for more specific analytic concepts in that context. This talk was given by Pietari Sarjakivi, NIXU Corporation: Safety and security could become important topics for OR analysts.

After these interesting talks, the CRITIS 2023 conference was closed with an award ceremony. The next conference, CRITIS 2024, will be organized by Stefano Panzieri at Universita Roma, fortunately together again in close cooperation with CODE. ■

Optimization problems within prediction attempts were treated by Farshad Farahnakian in his talk "Short and long-term vessel movement prediction for maritime traffic".

Grid topology and critical energy infrastructure

"Mapping and analysis of common vulnerabilities in popular web servers" was the title of the talk of Matyas Barocsai. In her presentation "Adaptable smart distribution grid topology generation for enhanced resilience", Natasa Gajic used a specific grid topology to optimize resilience.

After the coffee break, Peter Burgherr from Paul Scherrer Institute presented a plenary talk with the title "Hybrid threats and critical energy infrastructure in the context of the energy transition". The following plenary speech then focused on the ethical dimension of CI protection: In his talk "Ethics and the threat to infrastructure", Dr. Dr. Dieter Budde characterized several ethical dimensions and distinguished approaches.

Business continuity resilience and AI-based anticipation

In this specific context, Stefano Panzieri presented the approach "Managing uncertainty using CISIApro 2.0 Model" and Eveliina Hytönen "Business continuity building dynamic resilience". The other stream was centered around BCM models and OR-related solution concepts:

More information on CRITIS

https://www.laurea.fi/en/current-topics/events/critis-2023/

@ stefan.pickl@unibw.de

ALL FIG.: RI CODE / S. PICKL (2)

At the “Cyber Phoenix”, participants from three nations practiced defending against cyber attacks on critical infrastructure facilities, among other things.

FIG.: BUNDESWEHR / PIZ CIR

Report on the “Cyber Phoenix” Reserve Exercise at RI CODE

Three nations train for the emergency

During the second edition of the “Cyber Phoenix” exercise at the end of August, soldiers and reserve service personnel from Germany, the Netherlands and Australia trained together at CODE’s modern ICE & T Cyber Range. The five-day program included both individual and group exercises to practice defense against cyber attacks.

FOLLOWING THE SUCCESSFUL completion and positive experiences from the previous year, the Cyber and Information Domain Service (CIDS) conducted the reserve exercise “Cyber Phoenix” for the second time in the week from August 28 to September 1. In addition to reservists from Germany and the Netherlands, Australian soldiers also took part in the exercise for the first time. The scene of the action was once again “Camp CODE” – more specifically the modern ICE & T Cyber Range at the Research Institute CODE.

After several months of intense preparation, “Cyber Phoenix” began for the 36 participants in the briefing room on Monday morning. CODE Managing Director Marcus Knüpfer welcomed the soldiers from the three participating nations and introduced the team of trainers. After a briefing on the exercise scenario and the premises, the exercise participants then moved to their workstations in the Cyber Range to get familiar with the technical equipment and the working environment.

In the virtualized network environment of the Cyber Range, the multinational teams trained for five days in various scenarios on how to defend against cyber attacks on critical infrastructure facilities. The individual and group exercises focused primarily on cooperation in the investigation and analysis of attack patterns as well as the rapid restoration of the affected systems and services. In addition, suitable preventive measures were to be taken to prevent a re-attack.

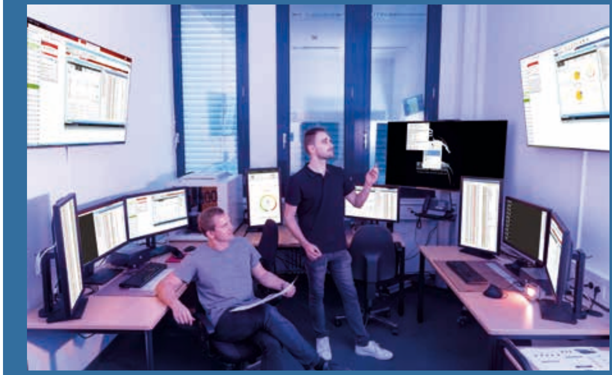
The representatives of the participating nations were also impressed, as they were able to see for themselves the progress made during the “Distinguished Visitors Day”. They expressed their great praise for the outstanding cooperation between the soldiers and once again underlined the importance of such cyber exercises. The participants also drew a consistently positive conclusion: The months of intensive preparation had once again paid off and ensured that the 2023 exercise was also a full success. ■

More about Cyber Phoenix

https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/trinationale-vorbereitung-auf-den-digitalen-ernstfall-5681178 (in German)

ICE & T's classrooms are made for team training.

ICE & T Cyber Range at RI CODE



Our trainers monitor the team progress, manage scenarios, and enable a unique learning experience.

The Cyber Range IT Competence Education & Training (ICE & T) at the Research Institute CODE is a comprehensive and flexible solution for real-world cyber security training. It provides a platform for learning and deepening competencies in Cyber Network Operations with a strong focus on teamwork. ICE & T also enables the evaluation of new cybersecurity products and approaches.

During training, cybersecurity scenarios are processed in a virtualized environment. The scenarios currently available at ICE & T are grouped in the categories Cyber Incident & Response Management (CIRM) Level 0-2, Supervisory Control and Data Acquisition (SCADA), and Penetration Testing (PT). Participants learn to analyze and defend against various attack patterns or apply PT methods in real system networks.

ICE & T is fully virtualized on a server cluster using VMware ESXi hypervisor. More than 400 virtual machines are used to enable multi-level scenarios as well as over 80 individual exercises and back-office services. The modular architecture also enables the integration of hardware components such as IoT and SCADA devices.

ICE T
IT Competence Education & Training

Further information

@ code@unibw.de

Information flyer "Cyber Range": https://go.unibw.de/85

ALL FIG.: UNIBW M / SIEBOLD

Quantum Technologies

Towards fault tolerance

“Recent advances in quantum technology bring us closer to a profound change in science and technology - a change that will have far-reaching implications for our economy, security and defense. These technologies could revolutionize sensing, imaging, precise positioning, navigation and timing, communications, data processing, modeling, simulation and information science.”

NATO Summary of NATO’s Quantum Technologies Strategy

IBM quantum chip Heron with 133 qubits.

EXPERIMENTAL CONTROL of quantum systems enables the processing of quantum information, in particular by exploiting the quantum properties of superposition, interference and entanglement.

Quantum information processing forms the backbone of quantum technologies: Quantum data from quantum sensors can be processed and temporarily stored in quantum memories. Quantum computers can be interconnected via quantum networks in distributed systems and connected to classical computers.

Today's quantum computers are still limited in their performance, however, as various sources of noise lead to errors. In general, the goal is therefore a fault-tolerant, universal quantum computer that can solve a large number of important problems. As we work towards this goal, we can already look for useful applications, new algorithms, and error mitigation techniques.

Here, as we better understand and mitigate the errors, we can begin to develop more powerful quantum algorithms. This will allow us to work on more relevant applications with each new generation of quantum computers.

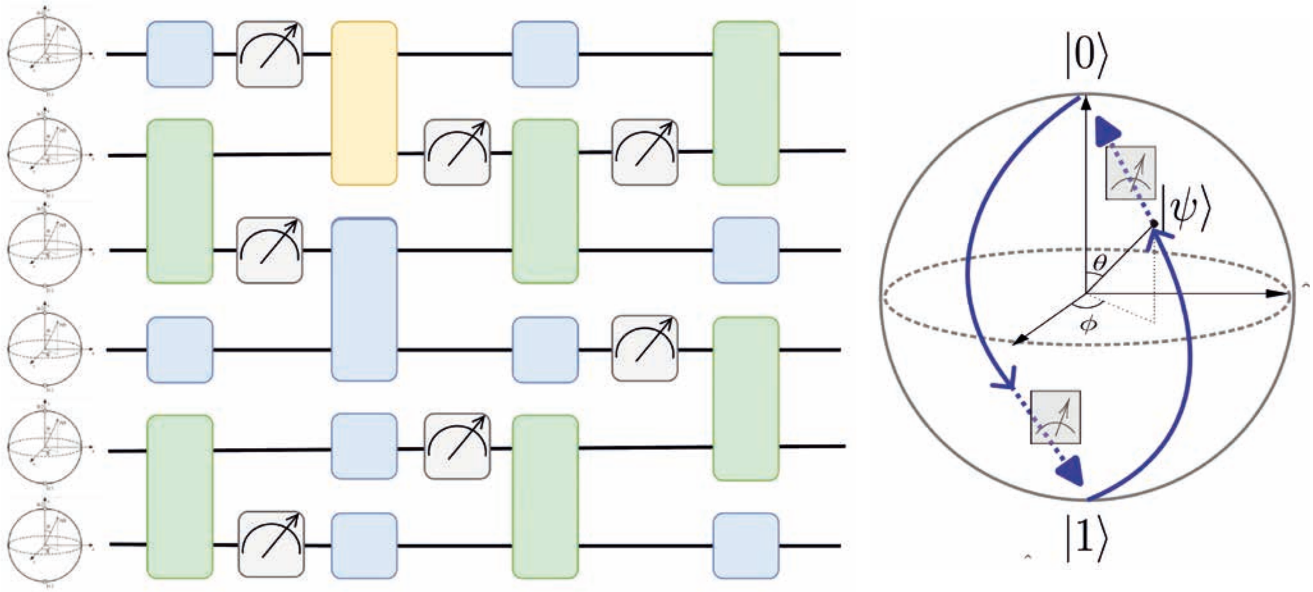
Current quantum computers are valuable for scientific research and development, which includes four basic areas.

First, the quantum computer is utilized as a "testbed" for quantum information processing issues: for example, the phase transition of entanglement dynamics induced by intermediate measurement or the process-

Broken cryptography is... not that unusual
Broken cryptography is... not that unusual
Munich Quantum Valley

Prof. Dr. Wolfgang Hommel spoke about the opportunities and risks of quantum computers to participants at the "Quantum Computing Meets Cyber Security" symposium in Garching in May 2023.

FIG.: IBM; MUNICH QUANTUM VALLEY / MIKKA STAMPA



Quantum circuits with intermediate measurements: The circuit thus consists of a deterministic unitary time evolution and the stochastic measurement that randomly projects to a quantum state |0> or |1>.

ing of quantum data. This knowledge can then be used in the development of quantum algorithms. Secondly, the investigation of error reduction techniques and error correction methods is conducted. Thirdly, the development of new algorithms such as randomization with mid-circuit measurements for simulation, optimization and machine learning. Fourthly, the identification of potential use cases.

Use cases for cybersecurity issues were discussed by experts from the fields of cyber security and quantum technology at a workshop we organized in May 2023 together with Munich Quantum Valley, entitled "Quantum Computing Meets Cyber Security". In particular, possible cyberattacks were discussed with the help of devices that use quantum technologies.

In addition, topics from applied research were passed on to students and employees of Bundeswehr-related service providers with the help of practice-oriented courses at Munich universities, through the supervision of final theses and at workshops, as well as through presentations at conferences and seminars. For example, the students were able to use the quantum computers to carry out experiments on quantum teleportation themselves

Experiments on questions of quantum information processing on the quantum computer

For quantum computing, it is typically necessary to initialize qubits in a quantum circuit, carry out controlled qubit interactions (a unitary time evolution using gates) and measure the resulting quantum states.

However, it is also possible to execute quantum circuits with periodic or random mid-circuit measurements of qubits and simultaneously process the resulting classical information. In the latter case, the circuit thus consists of a deterministic unitary time evolution and the stochastic measurement, which is randomly projected onto a quantum state.

Circuits with unitary time evolution with mid-circuit measurements exhibit a large number of dynamic phases that do not occur in a purely unitary time evolution with measurement at the end. A measurement-induced entanglement phase transition can thus be realized.

Quantum error mitigation techniques

Current quantum hardware is subject to various sources of noise, the best known of which are qubit decoherence, individual gate errors, and measurement errors. These errors limit the depth of quantum circuits we can implement, but even for short circuits, noise can lead to erroneous measured expectation values. Fortunately, quantum error mitigation provides a number of tools and methods that allow us to obtain more accurate expectation values from noisy quantum circuits with shallow depth. The error reduction techniques need to be tested on the hardware to reduce the hardware errors that occur when running quantum algorithms. Certain algorithms such as probabilistic error cancellation, for example, work in a similar way to noise reduction in headphones.

With classical post-processing and controlled approximations, the output of the original circuit can then be reconstructed. With this quantum-classical approach, small quantum computers can run an algorithm that requires more qubits than are available, and runtime and accuracy can be optimized until it is possible to apply quantum error correction.

Scaling the number of qubits in a quantum computer is a problem that still needs to be overcome. An interim solution is a scalable hybrid computing approach that combines conventional computers and various quantum computers using distributed quantum computing. Quantum circuits are broken down into smaller units so that they can be executed on smaller quantum chips.

Algorithms and applications

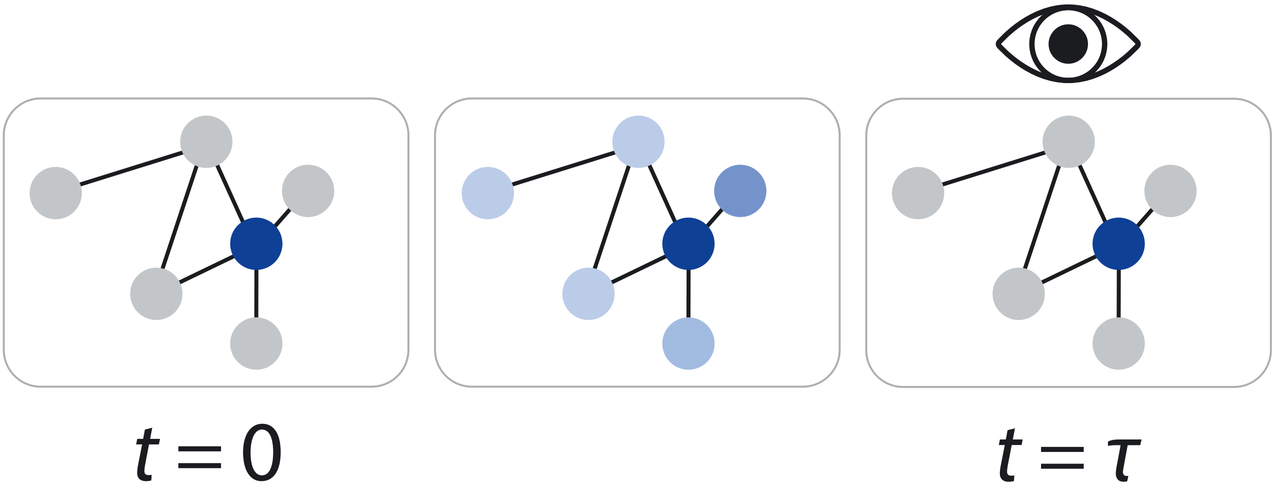
An important technique for developing quantum algorithms are quantum walks, which have become a universal computational model over the last ten years and were originally developed as a quantum version of classical random walks, in which the direction of the next step is determined by flipping a coin. Random walks are used in many areas, from biology and computer science to finance, which also applies to quantum walks. The laws of quantum information state that the development of an isolated quantum system is deterministic. Randomness only occurs when the system is measured and classical information is obtained. We investigate the possible application to problems from optimization and graph theory when quantum walks in different geometries are influenced by repeated stroboscopic measurements.

This new possibility of performing measurements during computation (“mid-circuit measurements”), such as on IBM quantum computers, opens up new perspectives in the field of algorithm development. Quantum circuits based on mid-circuit measurements have important applications, such as in quantum error correction, topological quantum computing, techniques for cutting and knitting circuits, reservoir computing or for preparing resource states in fault-tolerant quantum computing. Furthermore, with mid-circuit measurements and feed-forward operations, it is possible to overcome certain limitations of the circuit depth and the connectivity of the qubits on the qubit chip.

A large number of problems from logistics, supply chain management or cryptanalysis can be converted into an optimization task whose result is a state, a bit sequence or a distribution. For many of these problems, only approximate solutions can be found with the help of supercomputers. Quantum variation algorithms enable a learning-based approach. The parameters of the circuit (gate or pulse parameters) are found by optimizing a cost function. Quantum variation algorithms are continuously being improved in theory and experimental implementation, but new heuristic or approximation-based algorithms are also being developed.

Machine learning using quantum computers is an area of research that explores the interplay of ideas from quantum computing and machine learning. For example, we can find out whether quantum computing can reduce the time needed to train or evaluate a machine learning model, or we can use machine learning techniques to decipher quantum error correction codes, estimate the properties of quantum systems or develop new quantum algorithms.

With the help of quantum variation algorithms, quantum machine learning applications can be realized from quantum sensors,both for classical data and for quantum data.



ALL FIG.: RI CODE / S. TORNOW

Visualization of the return time of a “monitored quantum walk”.

These include quantum clustering, quantum Boltzmann machines, kernel methods, quantum convolutional neural networks, quantum support vector machines, quantum autoencoders and generative adversarial quantum networks. Kernel machine learning methods are ubiquitous in pattern recognition, with support vector machines being the best known method for classification problems, and can also be used as a quantum algorithm. The encoding of classical data into quantum states (quantum circuits) is called a quantum feature map. This feature map opens up the possibility of integrating the advantages of quantum information processing into machine learning algorithms. It can be assumed that we can maintain a quantum advantage if we choose a quantum feature map that is not easy to simulate with a classical computer.

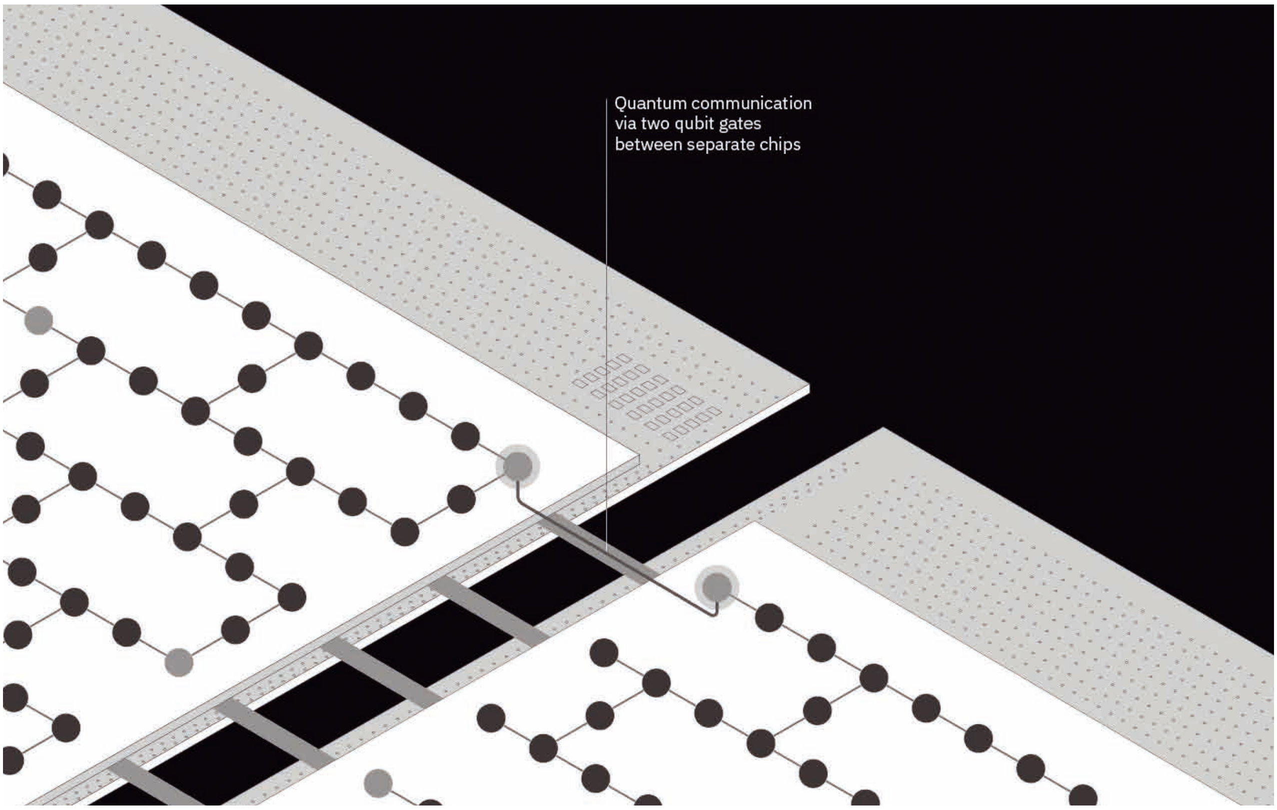
We investigate the predictive power of different combinations of quantum circuit architectures for the quantum feature maps. Finding a quantum advantage for the classification of real data is a major challenge, especially when it comes to heterogeneous data or large datasets that require more qubits than are available on current quantum computers. In our research, we are investigating quantum circuit architectures for data from different sources (data fusion), and the possibility of combining quantum chips to process larger datasets.

An exponential advantage has already been demonstrated in the field of quantum machine learning with quantum data: Instead of processing the quantum data with a classical computer, it can be briefly transferred to a quantum memory and evaluated by a quantum computer. To characterize the quantum state of the sensor, exponentially less data is then required compared to conventional processing. Another important application is the simulation of quantum materials.

However, quantum systems are not the only systems that are difficult to simulate. There are many important classical processes that could potentially be simulated more efficiently on a quantum computer, and if error tolerance is achieved through the successful use of error correction, algorithms already exist that could make this possible.

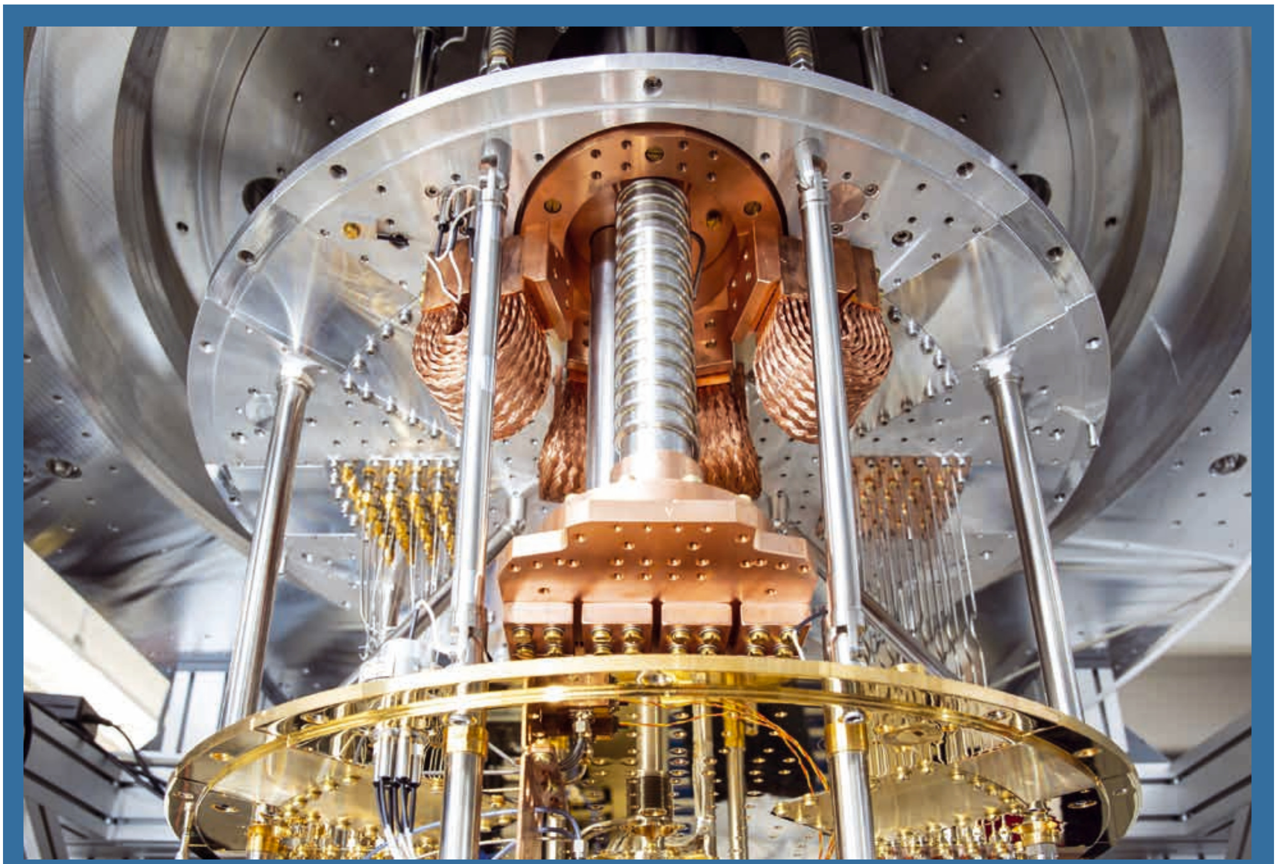
Outlook

The suppression and mitigation of errors is one of the central challenges for realistic applications in quantum computing. Error-corrected quantum computing, which enables new applications, is already emerging. Only recently, groundbreaking experiments have demonstrated scalable error correction and the possibility of quantum information processing with logical qubits.



Quantum communication between seperate chips.

FIG.: IBM; FZ JÜLICH / SASCHA KREKLAU



Quantum Computing

QUANTUM COMPUTING is a new paradigm that enables exponential speed increases over classical computing for certain computational problems. The computing operations are performed with qubits. A qubit is the smallest unit of information in a quantum computer. It is a quantum mechanical two-state system that can be in a superposition state of 0 and 1. Superposition enables interference effects that are central to quantum algorithms. Only when a measurement is made does the qubit enter one of the two states (0, 1). The measurement result can then be stored in a classical bit. With each additional qubit, the size of the state space available for a quantum algorithm doubles. This exponential scaling is the basis for the performance of quantum computers. Theoretical work has shown that, compared to the best known classical algorithms, certain structured problems can be computed exponentially faster with quantum algorithms.

Quantum computers promise enormous potential for efficiently solving some of the most difficult problems in the natural, economic and computer sciences, such as factorization, optimization, and modeling of complex systems. These problems are intractable for any current or future classical computer.

Today, many practical computational problems employ heuristic algorithms whose effectiveness has been empirically demonstrated. Analogously, heuristic quantum algorithms have also been proposed. However, empirical testing is not possible until the appropriate quantum hardware is available. With recent remarkable technological advances, it is now possible to test quantum algorithms and quantum heuristics on small quantum computers.

Contacts related to quantum computing at RI CODE

Dr. Sabine Tornow
sabine.tornow@unibw.de
+ 49 89 6004 7370

Dr. Wolfgang Gehrke
wolfgang.gehrke@unibw.de
+49 89 6004 7314

Quantum computing meets cyber security

At the "Quantum Computing Meets Cyber Security" symposium in Garching in mid-May 2023, experts from various fields came together to discuss cybersecurity risks in the age of quantum computers. The event was organized by Munich Quantum Valley, LMU Munich and RI CODE.

IN THE FUTURE, quantum computers are expected to be able to solve problems that go far beyond the capabilities of today's computers. However, these new possibilities also entail new risks - particularly with regard to the security of communication and information processing. Such potential uses of quantum technologies, such as for cyber attacks, must therefore be taken into account during development.

Interdisciplinary talks and discussions

In eleven presentations, cybersecurity issues and the threat of and defense against quantum-based cyber attacks were examined from various interdisciplinary perspectives.

These included contributions from experts in the fields of computer science, mathematics, cyber security and quantum physics.

Professor Dr. Wolfgang Hommel presented a security researcher's perspective on the risks and opportunities of quantum computers. In his presentation, the Executive Director of RI CODE outlined basic security paradigms, requirements and methods in connection with quantum computers, which will one day be integrated into more complex ICT infrastructures, and gave those who develop and design quantum computers an insight into the hopes and fears of the security community.

Moreover, the some 100 participants discussed applications from the field of quantum cryptography for secure communication technologies as well as issues of post-quantum cryptography and the need for security-by-design hardware.

All participants agreed that close cooperation between the various specialist disciplines is still necessary for a secure quantum infrastructure.

Active exchange and networking

The breaks in the program were also used by the participants for fruitful discussions. They continued the discussions over coffee and made new contacts for future collaborations or refreshed old ones. ■

The opportunities and risks of quantum computers were the subject of Prof. Dr. Wolfgang Hommel's talk in front of around 100 participants at the symposium in Garching.

BOTH FIG.: MQV / MIKKA STAMPA

As a memento of their visit, Colonel Beck (left) presented an artistic portrait of Albert Einstein to Professor Alt and Professor Geierhos.

BOTH FIG.: BUNDESWEHR / SEEGERT

First cyber awareness training hosted by JSEC

On March 16, 2023, the first cyber awareness training took place at the Joint Support and Enabling Command (JSEC) in the Wilhelmsburg barracks in Ulm. Under the guidance of Professor Dr. Florian Alt and Professor Dr. Michaela Geierhos from RI CODE, a total of around 250 NATO members received further training.

THIS YEAR'S FOCUS was on user-centered authentication and social engineering attacks as well as the detection of fake news and disinformation campaigns.

The aim of the event was to sensitize the international participants to the everyday threat of targeted manipulation. While social engineering is about influencing people to behave in certain ways, such as to disclose confidential information, disinformation campaigns can also lead to a massive weakening of trust in democracy and its constitutional principles as well as trust in freedom of expression. Using very illustrative practical cases, Professors Alt and Geierhos were able to give the soldiers not only current topics from their research on what is technically possible, but also valuable tips on what to look out for in order to protect themselves from this in both their professional and private lives.

As a souvenir of their visit, the two CODE professors received a portrait of Albert Einstein with the JSEC E^3 logo. The motto "Effective – Efficient – Enablement" embodies the vision of the JSEC. The three components are mutually dependent and generate a high degree of synergy, which can best be described mathematically with the third power, E x E x E = E^3, based on Ulm's most famous son and his formula E = mc^2.

Research mediation and awareness in the field of cyber security

From left to right: Prof. Dr. Arno Wacker, Prof. Dr. Bernhard Esslinger and Prof. Dr. Michaela Geierhos at the handover ceremony for the CrypTool project.

After 25 years, the open source project CrypTool – according to experts, the most widely used cryptography learning software in the world – has found a new home at the Research Institute CODE at the University of the Bundeswehr Munich. Prof. Dr. Bernhard Esslinger from the University of Siegen handed over the project management to Prof. Dr. Arno Wacker and Dr. Doris Behrendt in the context of the two-day CrypTool symposium.

ON MARCH 30 AND 31, 2023, more than 40 participants came together for the CrypTool Symposium at the Research Institute CODE. Current issues and the future development of CrypTool were discussed in numerous interesting presentations.

The highlights of the varied program included a talk by Dr. Lasry, whose name recently went through the press as the decryptor of Mary Stuart's letters, as well as contributions by Prof. Dr. Gregor Leander (Ruhr University Bochum) and Prof. Dr. Jürgen Fuß (University of Applied Sciences Upper Austria). Prof. Dr. Leander presented the CASA Cluster of Excellence and a special form of AI methods for cryptanalysis. Prof. Dr. Fuß gave insights into current research on quantum and post-quantum cryptography.

The CrypTool project (www.cryptool.org) is a collection of software applications, teaching and learning material on the subject of cryptography. The focus is on historical methods as well as applications that are used in modern IT environments. The crypto challenge website MysteryTwister (www.mysterytwister.org), which is based at the Ruhr University Bochum, is also linked to the project.

CrypTool was originally developed by Prof. Dr. Esslinger as an awareness tool during his time at Deutsche Bank. Under his leadership and with the help of numerous volunteers, students, researchers and challenge solvers from all over the world, it has since undergone continuous further development. CrypTool is characterized in particular by its high technical quality and its open source approach, which enables users to use the software free of charge.

In 2019, the technical infrastructure of CrypTool was already moved from Kassel to Munich. Now the content management has also been handed over to the Research Institute CODE and Prof. Dr. Wacker's Chair of Privacy and Compliance. Dr. Behrendt will be responsible for the further development and maintenance of the CrypTool project in the future. ■

Prof. Dr. Gregor Leander spoke at the symposium about the CASA Cluster of Excellence and AI methods for cryptoanalysis.

BOTH FIG.: RI CODE / B. BELLGRAU

CODE hosts its first OSINT forum

On November 8 and 9, 2023, around 60 OSINT experts met in Munich to discuss current technical topics and possible future applications.

OPEN SOURCE INTELLIGENCE (OSINT) is becoming increasingly important in view of the challenge of processing a constantly growing volume of information that is publicly accessible and can be relevant to a wide range of issues. A reasonable integration of OSINT not only requires technical solutions for processing the amount of data. It also requires well-trained specialists who can evaluate the data and establish suitable processes and procedures.

Due to the relevance and complexity of the topic, the Research Institute CODE, in cooperation with ESG Elektroniksystem- und Logistik-GmbH and PD - Berater der öffentlichen Hand GmbH, organized and hosted an OSINT forum for the first time. The aim of this event was to facilitate the exchange and networking of civil and military security experts with OSINT specialists from research and industry.

> “Extracting usable information from open data is an enormous potential of OSINT that we must utilize.“
>
> *Prof. Dr. Michaela Geierhos, Technical Director of RI CODE*

The OSINT Forum was officially opened on November 8 in Munich by Prof. Dr. Michaela Geierhos, Technical Director of CODE and Professor of Data Science.

Together with her colleague Prof. Dr. Eirini Ntoutsi, since August 2022 Professor of Open Source Intelligence at the University of the Bundeswehr Munich, she represented the scientific perspective on the topic.

“Extracting usable information from open data is an enormous potential of OSINT that we must utilize,” said Geierhos. The fields of application of OSINT in the public sector, but also in industry, are just as versatile as its potential uses. It is thus obvious that expertise needs to be pooled and networking across organizational structures needs to be improved.

“It is therefore a central concern of CODE to provide a forum where urgent issues in the field of OSINT can be discussed regularly and exclusively in the future,” added the Technical Director. ■

The first OSINT forum was officially opened by Stefan Vollmer (ESG), Prof. Dr. Michaela Geierhos (FI CODE) and Louis Jarvers (PD) (f. l. t. r.).

FIG.: RI CODE

Bundeswehr’s Head of CIT Department visits CODE

Lieutenant General Michael Vetter, Head of the Cyber/Information Technology (CIT) Department and Chief Information Officer at the German Federal Ministry of Defence (BMVg), met with CODE scientists during his visit to Munich on November 20, 2023, and learned about current advances in cyber security and quantum technology research.

AFTER MEETING WITH the CODE management, selected chairs and research groups gave Lieutenant General Vetter an insight into their research topics. Two newly appointed CODE professors, Prof. Dr. Marta Gomez-Barrero and Prof. Dr. Daniel Slamanig, also introduced themselves. Gomez-Barrero has held the professorship for Machine Learning since October. Slamanig was appointed Professor of Cryptology at the beginning of November. There was also an update on developments in the field of quantum technologies and the latest activities in the field of software-defined defense, in which CODE is involved.

Insights into CODE labs and Cyber Range

The dtec.bw research project MuQuaNet, which aims to set up and operate a quantum-safe network, was also presented to the Lieutenant General. During a tour of the MuQuaNet lab, Vetter was given an insight into the status of the work. He also visited the BehaVR Lab of Professor Dr. Florian Alt, who is conducting research there with his team on issues such as behavioral biometrics. The tour of the research institute ended in the Cyber Range, where the team of trainers gave the guest from the BMVg an insight into the latest developments and exercise scenarios used to train specialist personnel at RI CODE.

Time for personal discussions with exercise participants

During his visit to the simultaneous “Army Cyber Spartan 2023” exercise, Lieutenant General Vetter was able to see for himself the high quality of the training and further education that takes place at CODE. This year, in addition to numerous international teams, an all-student team from UniBw M remotely took part in the British Army’s cyber defense exercise from the reachback at RI CODE. For one week, the ten-person group focused on training live-fire defense and threat hunting and achieved a place in the top four in the end. Following the visit to the exercise, the General took time for personal discussions with the exercise participants and other soldiers from the cyber and information space sector. ■

Selected chairs and working groups gave Lieutenant General Vetter an insight into their current research topics at CODE.

After the visit to the exercise, General Vetter took time for personal conversations with the soldiers.

ALL FIG.: UNIBW M / SIEBOLD

General Sverre Diessen, Jackie Eaton, Donna Wood, Stefan Pickl and Colonel Matthias Kinkel (f. l. t. r.).

FIG.: RI CODE / S. PICKL

Stefan Pickl receives Excellence Award for his work at the NATO Think Tank

For his comprehensive research contribution to the future impact of COVID-19 on the NATO alliance, Prof. Dr. Stefan Pickl from the University of the Bundeswehr Munich (UniBw M) was honored with the Excellence Award by the NATO Science and Technology Organization (STO) in Harstad, Norway, at the end of May 2023. Prof. Dr. Stefan Pickl worked in the international working group "STO Specialist Team SAS169" for more than two years, which dealt with special vulnerability analyses and process optimizations in the context of the corona pandemic.

WITH THE EXCELLENCE AWARD, the STO recognizes outstanding contributions in selected panel research activities every year. This was also the case in 2023. Prof. Dr. Stefan Pickl from the Institute for Theoretical Computer Science, Mathematics and Operations Research at the UniBw M and the Research Institute CODE received the Excellence Award for his work in the special SAS panel "The future impacts of COVID-19 on the Alliance".

Prof. Dr. Stefan Pickl is also the German representative on NATO's SAS Board and regularly participates in international working groups. This is already the second time that a working group with his participation has been honored. "I am particularly grateful for this award, as the working group had to be established very quickly and was only able to work together internationally under difficult conditions, not least due to the pandemic", summarizes Prof. Pickl.

Prof. Pickl's research group has been working closely with the WHO for several years, and Prof. Dr. Stefan Pickl is also on the scientific advisory board of the "Healthcare System Engineering" program at the University of Central Florida. As part of NATO's Science for Peace Program, his COMTESSA working group developed an IT-based decision support platform in the context of the international MASSAI project (Management of Mass Casualty via an Artificial Intelligence-Based Platform), and its concept was also incorporated into the extensive analyses of the SAS working group. ■

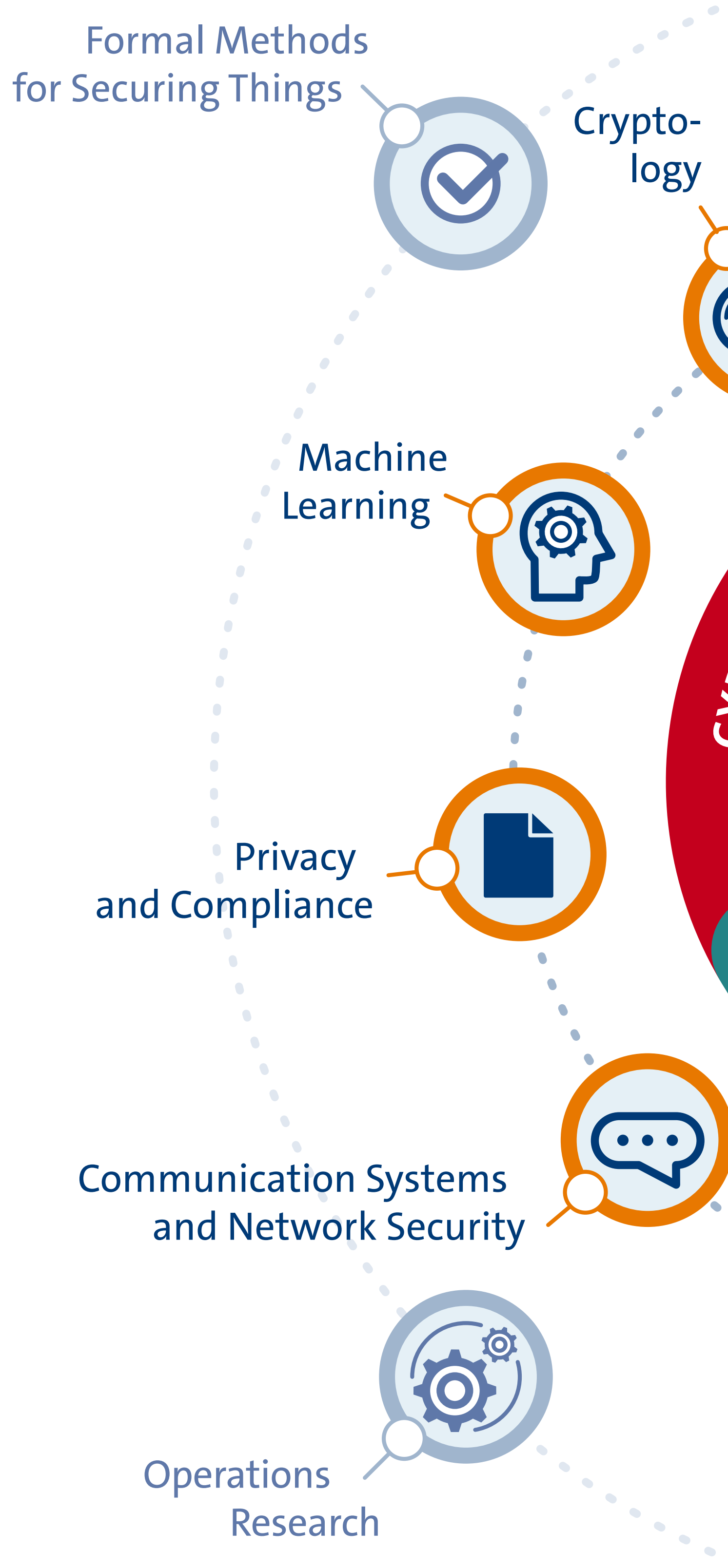
FIG.: ADOBE STOCK / ESI

Research

Portraits and Projects

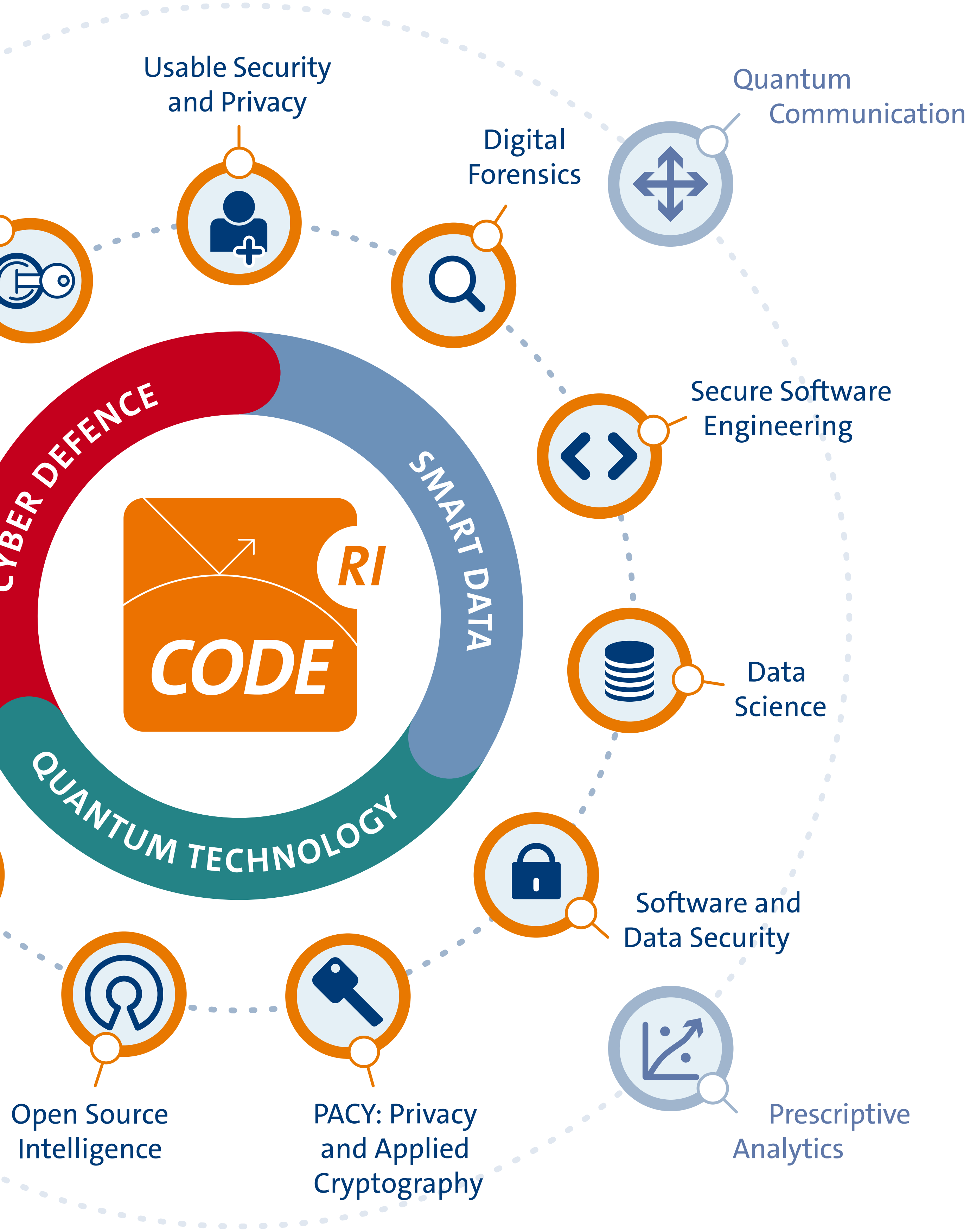
Research at RI CODE

Currently, there are 51 third-party funded projects being carried out in various research groups at the Research Institute CODE. 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.



Formal Methods for Securing Things
Crypto-logy
Machine Learning
Privacy and Compliance
Communication Systems and Network Security
Operations Research

FIG.: TAUSENDBLAUWERK.DE


Usable Security and Privacy
Digital Forensics
Quantum Communication
Secure Software Engineering
Data Science
Software and Data Security
Prescriptive Analytics
PACY: Privacy and Applied Cryptography
Open Source Intelligence
CYBER DEFENCE
SMART DATA
QUANTUM TECHNOLOGY
RI
CODE

Prof. Dr. Florian Alt

Research Group Usable Security and Privacy

The research group Usable Security and Privacy, headed by Prof. Dr. Florian Alt, explores human behavior in security-related systems. In particular, the group looks into the role of security and privacy in user-centered design processes and investigates how secure systems can be better adapted to the way in which users interact with computing devices.

THE USABLE SECURITY AND PRIVACY GROUP was founded in 2018 and conducts research at the crossroads of Human-Computer Interaction, Cybersecurity, and Privacy. With his team, Prof. Dr. Florian Alt investigates how researchers and practitioners can be supported in considering security and privacy needs already during user-centered design processes. The ultimate goal is to better blend security and privacy mechanisms with the way in which users interact with technology in everyday life.

Research areas and methodology

The research group focuses on a variety of different research topics. These include the study of human behavior and physiological responses in security-critical situations, the development of new as well as the improvement of existing security and privacy mechanisms based on human behavior and physiology (especially gaze), the study of novel threats posed by ubiquitous technologies and the development of appropriate protection mechanisms, and the exploration of approaches to improve the understanding and behavior of users in security-critical situations. Specific application areas include smart home environments, social engineering, social biometrics, and mixed reality.

As part of its research, the group draws on research methods that are commonly known from human-computer interaction and continues to evolve them. These methods include user-centered design and iterative prototyping. The work has a strong human-centered focus, which makes empirical approaches a fundamental part of the group‘s research. To understand behavior and evaluate new approaches, studies are conducted both in the lab and in the field.

Infrastructure and publications

The group operates in a human-computer interaction lab, equipped with a state-of-the-art indoor positioning system, stationary and mobile high-end eye trackers as well as other physiological sensors, thermal cameras, and augmented as well as virtual reality devices. In addition, the group is currently setting up a testbed, allowing users’ behavior and physiological responses to security incidents to be investigated in the real world.

Together with his team, Prof. Dr. Florian Alt has published over 300 DBLP-listed scientific articles and won 18 awards in leading scientific venues of his field. The research of the group received funding from the German Science Foundation (DFG), the Digitalization and Technology Research Center of the Bundeswehr (dtec.bw), the Federal Ministry of Defence (BMVg), the Bavarian State Ministry for Education and Science, the Humboldt Foundation, the DAAD, Google, and the BMW Group.

Development of the Research Group in 2023

In 2023, the research group Usable Security and Privacy included 13 employees and five research assistants besides Prof. Dr. Florian Alt. Among the research group‘s scientific staff are seven Ph.D. students and four postdocs, who contributed to 23 publications in 2023.

Prof. Dr. Florian Alt

@ florian.alt@unibw.de

☎ +49 89 6004 7320

www.unibw.de/usable-security-and-privacy-en

The Usable Security and Privacy Group was well represented at the ACM CHI Conference on Human Factors in Computing Systems 2023 – the largest and most well-known HCI conference.

FIG.: ISTOCK / PHOTOTECHNO; RI CODE / ALT

Project PriMR

User interfaces for communication and control of privacy aspects in mixed reality

Mixed reality headsets collect data about their active users (e.g.: usage data, movement data, heart rate) and about people in the environment (passive users). PriMR addresses how active and passive users can be sensitized to the impact of MR technology on their privacy and how they can be supported in making informed decisions regarding data collection, processing and sharing.

Data collection and privacy in mixed reality

Mixed reality (MR) headsets facilitate numerous new applications, including leisure, work, education and marketing activities. With MR, users can immerse themselves in a virtual world or expand their view of the real world with virtual content. To achieve this, MR headsets use sensors that can capture, process and share sensitive data with third parties. Modern headsets allow access to behavioral data (hand and body movements, gaze), physiological data (EEG, heart rate), and contextual data (tracking room, passive users). Such data can be used to derive information about demographics, health status and disabilities. It is obvious that such data is sensitive. While sensors are required to enable tracking and interaction, the data collected can be misused. This poses a challenge as access to the data is necessary to create an immersive user experience. At the same time, it is important to enable users to protect their data from unintended use.

PriMR: Privacy awareness and control for users

The PriMR project investigates how user interfaces for privacy control can be developed for MR. The core challenges are (1) how to inform active and passive users about the privacy implications of using MR technology and (2) how to support them in making meaningful decisions regarding data collection, processing and sharing. As MR is used in numerous environments, supports a growing number of applications (gaming, office, education), continuously integrates novel sensors, and involves users with different capabilities, the following questions arise: How can MR user interfaces raise awareness of what data is collected, processed and shared? How can passive users be informed by MR users about ongoing tracking and how can they be granted control over their data? How can MR user interfaces support efficient consent to data protection? How can researchers and practitioners be supported in the privacy-compliant design of MR applications? The PriMR project is an important step towards making data protection an integral aspect in the development of MR applications.

Prof. Dr. Florian Alt

florian.alt@unibw.de

☎ +49 89 6004 7320

https://www.unibw.de/usable-security-and-privacy-en/research/projekte/primr_dfg

Funded by:
German Research Foundation (DFG)

PriMR investigates how users can be sensitized to the impact of mixed reality technology on their privacy.

FIG.: ISTOCK / METAMORWORKS

Project User-Centered Biometric Interfaces

Improving users' literacy on and agency over biometric authentication

The machine learning models underlying biometrics authentication methods (e.g., fingerprint, face-recognition or behavioral biometrics) act as a black box to the users, making their decisions hard to understand and leading to biases. This project enhances existing interfaces with biometric systems and proposes new ones with the aim to facilitate user literacy and agency over their functionality.

Usability issues of secret-based authentication

Authentication has become an essential part of our daily lives. Examples include using authentication tokens like keys to enter a building or vehicle, or the use of passwords, PINs, and patterns to access digital accounts and devices. However, such traditional approaches are starting to reach their limits, as the ever-increasing number of required authentications strains both users' memory and time.

Biometric authentication mechanisms

Biometric methods make use of unique patterns in user physiology or behavior for the purpose of authentication and are proposed as a potential solution. They do not require mental effort, cannot be stolen or forgotten, and can operate in the background with no active user engagement required. However, biometrics also come with drawbacks: Their underlying machine learning models mostly act as black boxes to users while at the same time being prone to systemic biases and inconsistent recognition performance. Users get little insight into what constitutes model decisions, let alone control over the authentication mechanism that is to protect their data.

Enhancing users' literacy and agency

This project takes a user-centered approach to enhance existing interfaces with biometric systems and propose new ones with the aim to facilitate 1) user literacy and 2) agency over the recognition process. In particular, we answer these questions: What are user needs and how can they be addressed through the design of biometric interfaces? How can users be supported to acquire biometric literacy through biometric interfaces? How can biometric interfaces be leveraged to extend user agency?

User-centered biometric interfaces

We conducted a large variety of studies to understand user preferences and needs with regard to biometrics and designed biometric interfaces to support users in understanding influencing factors on their authentication and take control if desired. Moreover, we propose solutions that can help users gain personalized insights into the performance of a biometric system, understand and react to contextual factors influencing it, and anticipate model decisions through introspection into its state. We also show that it is possible to gain agency over a biometric method that does not inherently offer interfaces.

The functionality of biometric authentication methods (e.g., fingerprint, facial recognition or behavioral biometrics) is often not clear to users.

FIG.: ISTOCK / BLUE PLANET STUDIO

Overall, we explored how biometric interfaces could look like, how they could improve interaction with biometric systems, and if they can contribute to an informed and secure use of biometric authentication.

Lukas Mecke

@ lukas.mecke@unibw.de

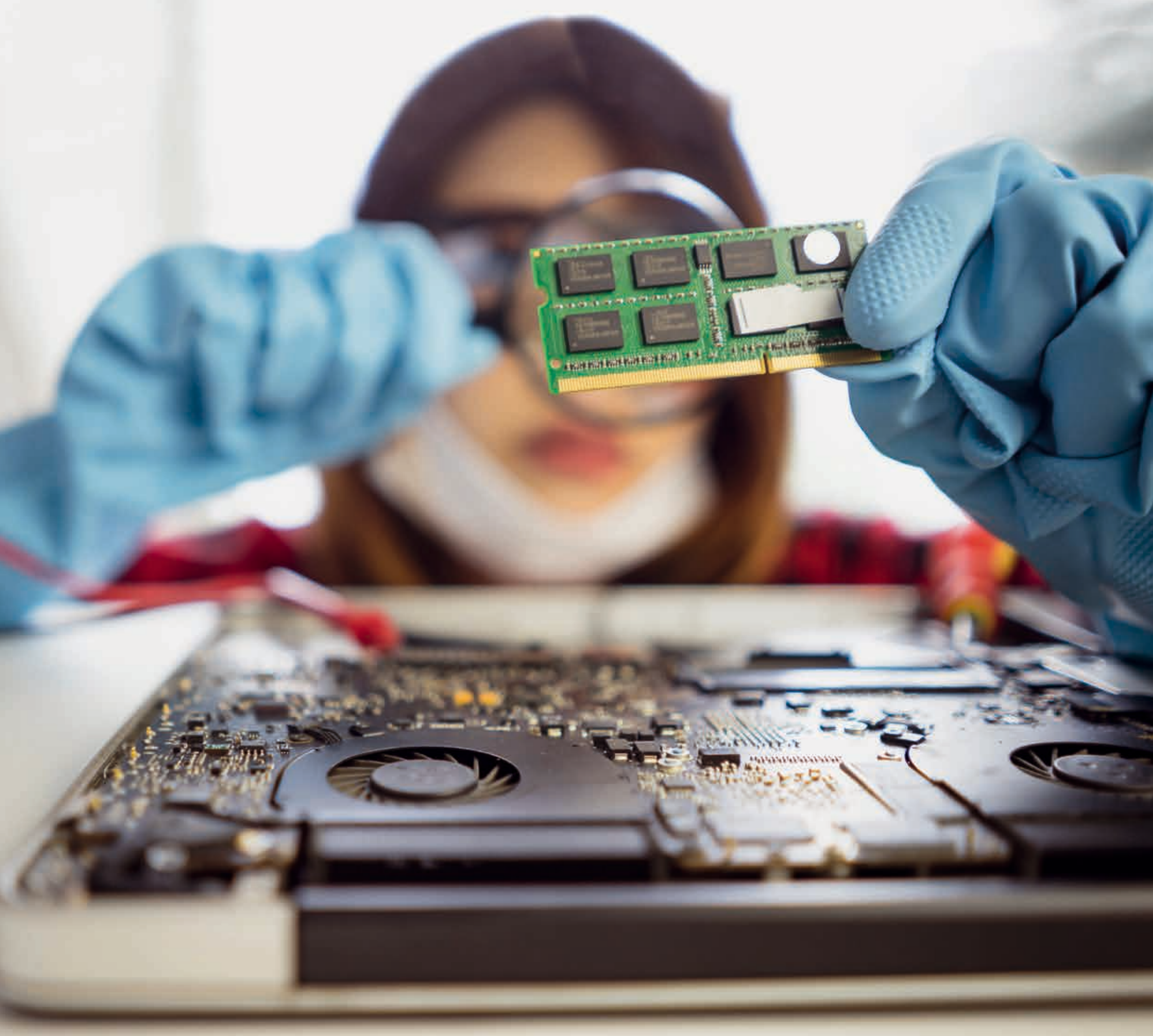
☎ +49 89 6004 7323

www.unibw.de/usable-security-and-privacy-en

Prof. Dr. Harald Baier

Digital Forensics

Due to increasing digitization and subsequent cybercriminal activities, the need for digital forensics competencies is growing too. The main research areas of the Professorship of Digital Forensics address the handling of bulk data in IT forensic investigations, the generation of synthetic datasets to assess IT forensic tools, anti-forensics, and main memory forensics.



DIGITAL FORENSICS, as the digital equivalent of the classic forensic disciplines, always comes into play when an answer to a question of doubt is sought in connection with an IT system. A case in point would be when a remote-controlled drone is used to transport drugs, but during transport the drone crashes onto the property of a bystander. When called to help, the police take over the drone and are supposed to clarify the questions of doubt as to who was piloting the drone and what routes it was flying. To do this, the supporting IT forensic experts secure the drone's data media, analyze them, and try to provide answers to the questions of doubt.

Seeking access

An IT forensic investigation is associated with numerous challenges, which the Professorship of Digital Forensics deals with. A first important challenge is the question how data can be secured and analyzed, especially that from innovative IT devices such as drones or cars. The background to this is that these devices often only offer unknown interfaces for access and that data storage is dependent on the manufacturer in terms of partitioning, the file system, and the file format.

Searching for training data

A second important challenge is the accuracy of IT forensic tools, meaning that they should work as specified. This requires standardized test datasets. For these, the digital traces to be detected are known a priori and matched against the detected traces by the respective tool. However, such datasets are not sufficiently available to the community.

Throwing sand in the gears

A third important task is dealing with anti-forensics, i.e., all measures taken by attackers to cover up or destroy their tracks. Anti-forensics have always been used by criminals – for example, a burglars wear gloves to avoid leaving telltale fingerprints. In digital forensics, it is important to understand and detect anti-forensic methods used by attackers.

👤 Prof. Dr. Harald Baier

@ harald.baier@unibw.de

☎ +49 89 6004 7345

🌐 www.unibw.de/digfor

One challenge of IT forensics is to secure and analyze data.

FIG.: ADOBE STOCK / NOPPONPAT, MICROGEN

Investigation of DIY Drones

IT forensic data analysis: DIY drones in the focus of law enforcement

In addition to commercial drones, the dynamically growing market for unmanned aerial systems also offers a wide range of kits that can be used to build so-called DIY drones. Drones are also increasingly being used for criminal activities, for example to prepare and carry out drug smuggling or theft offences and can be customized to meet specific needs.

DRONES can be divided into different categories according to characteristics such as the size, weight, span, intended use or even regional legislation.

Prosecution

The number of drones used in investigations in connection with the IT forensic preservation and examination of digital evidence is constantly increasing.

To date, the majority of drones seized have been commercial drones, which are usually processed using standard commercial software for securing and analysis.

DIY drones

However, manufacturers of forensic software do not pay attention to the area of do-It-yourself drones. These flight systems are individual parts or kits that can be customized. Drones can be highly customized in terms of functionality and performance or can be less expensive if lost. DIY drones can be used in cases such as to circumvent no-fly zones or spy on properties.

These customization options mean that commercial software packages often cannot be used to secure and investigate DIY drones, because they do not offer the option of backing up or analyzing the new interfaces and data formats.

DIY drone of the Digital Forensics research group, which is used in the FOCUS project together with other reference devices for data generation.

Digital forensics

The data generated on the seized drones can be helpful in solving criminal offences.

During the use of a drone, data such as flight altitude, speed, take-off and return locations, defined flight routes or even recorded image and video material can be secured.

Digital forensics methods can be used to track down and read out the data memories of drones. This can provide law enforcement authorities with important investigative leads.

Project FOCUS

The Forensic Examination of DIY Drones (FOCUS) addresses the investigation of two scenarios:

1. Discovery of a drone in connection with criminal activities and
2. Loss of a drone during use by security authorities.

The research focuses on extracting and analyzing stored data. Scenario one is aimed at securing evidence. Scenario two attempts to prevent unauthorized access to the data.

The aim of the project is to develop recommendations for the use of DIY drones and tool chains for forensic investigations that can be used for criminal prosecution.

HptFw d. R. Mario Winkler, M. Sc.

@ mario.winkler@unibw.de

☎ +49 89 6004 7346

www.unibw.de/digfor

Funded by: BMBF

FIG.: RI CODE / MARIO WINKLER

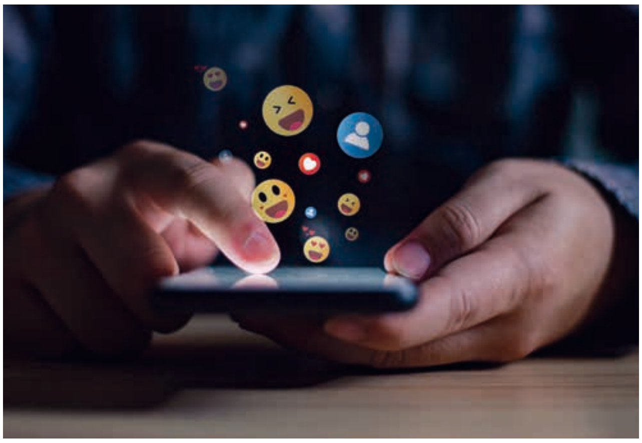
To possess or not to possess …

… that is the question: Illegal WhatsApp stickers on Android and their prosecution.

WhatsApp stickers are a popular mix of emoticons and user-created images or videos. They are not subject to any authoritative control but are automatically shared from peer to peer in chats. As a result, they can go viral – not just the funny ones, but also the illegal ones. This puts users in the unfortunate position of having incriminating media files on their device without knowing or wanting to, and law enforcement in the unexpectedly difficult position of distinguishing perpetrator from victim.

From funny to illegal

Meta introduced stickers to WhatsApp in 2018, and since then, the ease of creating them has gradually increased. At the moment, Meta makes it possible for all users to create their own stickers from any image in an instant. This seems like good news. After all, stickers are mostly shared for legitimate purposes. However, users also share stickers with illegal content, such as Child Sexual Abuse Material (CSAM) or Nazi propaganda. On the one hand, law enforcement and the courts have been confronted with cases where users have unknowingly received CSAM in ordinary group chats. On the other hand, there are cases where users have engaged in the very activities that the law is designed to punish.



The prosecution of illegal WhatsApp stickers is a challenging task.

FIG.: ISTOCK / CHOOCHART CHOOCHAIKUPT

Prosecutable possession?

These cases usually revolve around the question of whether the user is in possession of such an illegal sticker. Interestingly, the concept of possession is easy to translate to the digital world, but hard to decide. In most jurisdictions, possession means that a person has actual control over an object, in this case a sticker, and that the person knows of its existence. Some laws also require intent as a condition of possession. However, this means that it is possible to use technical ignorance as an argument against having actual control or knowledge of a file. Obviously, it is not the intent of the law that intentional interactions with CSAM go unpunished for allegedly technically unsophisticated individuals.

Results enable prosecution

To provide valuable insights for law enforcement and digital forensics practitioners, the professorship for Digital Forensics conducted a thorough digital forensic analysis of the entire lifecycle of community-created stickers. Most importantly, the results clearly show that simply finding a sticker on an Android device is not sufficient to infer possession, as a sticker can be acquired without knowledge of its existence. Furthermore, the research provides a detailed guideline for law enforcement to convict an offender of distributing or possessing illegal stickers.

This research will hopefully contribute to ongoing efforts to combat the distribution of illegal content through messaging apps, while also helping innocent people caught in the middle.

Samantha Klier, M.Sc.

@ samantha.klier@unibw.de

☎ +49 89 6004 7346

🌐 https://www.unibw.de/digfor

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

The research group headed by Stefan Brunthaler focuses on language-based security, an area that investigates the use and applicability of language-based transformations to secure vast amounts of software in a way that is automated, transparent, and effective. A key aspect of these techniques is that it offers unparalleled scalability, as evidenced by the ability to compiler hugely complicated software such as web browsers.

THE Munich Computer Systems Research Laboratory (µCSRL) directed by the Chair of Secure Software Engineering conducts world-class research in computer security by coming up with novel defences that mitigate advanced attacks, primarily focusing on code-reuse attacks. By leveraging our expertise in fundamentals of programming, particularly in compiler technology, we tackle challenging and important problems in programming languages, as well as security and privacy through our focus on language-based security. Paraphrasing Clausewitz, we believe that language-based security is the continuation of compiler construction by other means.

The past year continued our successful growth along multiple dimensions, thereby ensuring µCSRL's visibility and ability to continue tackling challenging problems.

Our compiler-driven technique to mitigate address-oblivious code reuse (AOCR) was accepted for publication in the prestigious 18th European Conference on Computer Systems (EuroSys). Besides publication, we also gave a presentation when the conference took place in Rome.

In September of 2023, the whole research group attended the 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung (KPS 2023), and gave presentations on a variety of research topics currently pursued at µCSRL: fuzzing, optimization of Web Assembly (WASM) interpreters, first steps of our international collaboration with KU Leuven and EPFL in the Dependable Production Systems project, and our new technique to prevent Counterfeit Object-Oriented Programming (COOP) through compiler-driven support for preserving object-integrity in C++ programs.

Besides attending KPS, the research group also attended EuroS&P in Delft, as well as the ACM Computer and Communications Security conference in Copenhagen, Denmark.

From a project perspective, we are happy to report that our project with Airbus was not only finished on time, but that we were also able to complete *all* of the planned milestones to the full satisfaction of Airbus.

People-wise, we are happy to see continuous growth: Matthias Bernad chose to join µCSRL after his successful completion of his Master's degree at TU Wien in June of 2023. In addition, we supervised several bachelor and master students, one of which spent part of his MSc research at the University of California, San Diego.

In 2023, Prof. Dr. Brunthaler was invited to serve on the program committees of the Symposium on Network and Distributed System Security (NDSS 2024 in San Diego, USA), the 2024 ACM SIGPLAN International Conference on Object-Oriented Programming Systems, Languages, and Applications (OOPSLA 2024 in Pasadena, USA), the IEEE European Symposium on Security and Privacy (EuroS&P 2024 in Vienna), and the 2024 Workshop on Principles of Secure Compilation (PriSC 2024, co-located with POPL 2024 in London, UK). As of 2023, Prof. Dr. Brunthaler acts as the area chair for System Security at the *Journal of Systems Research* (JSys).

The µCSRL research group received funding from the German Ministry of Defence, and the Austrian Research Promotion Agency of the State of Upper Austria.

Prof. Dr. Stefan Brunthaler

@ brunthaler@unibw.de

☎ +49 89 6004 7330

www.unibw.de/ucsrl-en

FIG.: ISTOCK / DE M10

Looming Danger of Supply-Chain Attacks

Known defenses found to be impotent

Supply-chain attacks, in analogy to the study of kinetic attacks, are *indirect*. To hit a target, they attack or undermine underlying infrastructure, such as compilers and interpreters, or build tool chains. Once a victim updates their infrastructure, attackers have almost won.

Trust noone!

In 1984, Ken Thompson gave a talk aptly named "Reflections on Trusting Trust", which subsequently became a cornerstone of required reading for software security courses. The key problem addressed by Ken Thompson is that indirect attacks are not only possibly but incredibly powerful. As an example, Thompson changed a compiler such that it would insert a backdoor every time it compiles a passwd program, which is used to check a password at login time. As a result, whenever this program was compiled, a backdoor would be present, breaking OS authentication barriers. As an additional subterfuge, Thompson described how to hide the backdoor inserting code: Since a compiler is needed to compile itself, Thompson added additional code that would detect when it compiled itself and would silently propagate the backdoor insertion logic. Consequently, the source code for inserting the backdoor could be removed, meaning that no investigation of a compiler's source code could reveal the backdoor. Reflections on trusting trust thus clearly delineates the limits of trust as well as clear and present danger emanating from indirect attacks.

Fast forward to 2024

Over the past few years, supply-chain attacks have gained attention, primarily through a series of widespread attacks, such as SolarWinds. Although known supply-chain attacks differ in their inner workings, they clearly pinpoint the brittleness of modern software. A hodgepodge of proprietary and open source 3rd party libraries as well as variety of system dependencies for both hard- and software.

This hodgepodge situation is further exacerbated by engineering and manufacturing companies' heavy reliance on suppliers. Often, the company integrating supplied components has no way of enforcing specifics, such as which compiler or programming language to use. In consequence, manufactured goods provide a huge attack surface for indirect, supply-chain attacks.

To shed light on these problems, industry and academia alike have proposed to borrow a concept of physical manufacturing, namely so-called bill of materials, which detail what components are inside a machine. The borrowed concept is referred to as software bill of materials, denoted by the abbreviation SBOM. A variety of standards exist, and they will be produced by a build tool or process to indicate which components a piece of software contains or relies on.

What follows from these events

Considering both perspectives, reflections on trusting trust and the ongoing trend of software bill of materials, it follows that SBOMs will likely improve the present situation that renders any piece of software as a black box. At the same time, however, it should be clear that through indirect attacks in the vein of Thompson, SBOMs will remain impotent.

Upon closer analysis of today's software landscape, combined with a purview of current processes in mechanical engineering, we conclude that manifold changes are required to meet the clear and present danger of supply-chain attacks.

Procurement processes need to consider the information available to suppliers, such that double indirection via a supplier's supplier becomes less probable. The same observation holds for outsourcing of software development work. During software construction or building of complex software pieces, blind trust in utilities is not commensurate with the potential problems through supply-chain attacks. Similarly, certification entities that certify software for use in critical infrastructure need to update their processes such that expensive and time-intensive recertification become obsolete.

👤 Prof. Dr. Stefan Brunthaler

@ brunthaler@unibw.de

☎ +49 89 6004 7330

🌐 www.unibw.de/ucsrl

Fast and Efficient Binary Component Identification

Reverse engineering efforts to identify binary components in programs is a tedious, error-prone task. Time and again, reverse engineers have to analyze programs only to find that a certain piece of binary code corresponds to a known, benign function. The resulting friction and waste of time poses a significant obstacle to reverse engineering.

Binary component identification

A program in binary representation is merely a blob of seemingly random sequences of zeroes and ones. Although meaningful and – hopefully – reasonable to the computer executing the program, to a human the zeroes and ones just mean gibberish. To analyze a program in binary representation, humans therefore perform a series of steps to incrementally attach meaning, i.e., semantics, to parts of the program. As a first step, binary programs are typically disassembled, meaning that the zeroes and ones are replaced by a textual representation of the native machine instructions, such as a MOV RAX, RBX. Although this representation is legible and meaningful, isolating larger parts remains tedious. As a potential next step, decompilation intends to produce high-level source code, for instance C code, out of many single, isolated native machine instructions. Decompilation itself, however, is fundamentally undecidable, so there are sequences that cannot be decompiled effectively to C. The present state of the art also suffers from a deluge of other hard problems, such as control-flow, data-flow, and type recovery. All of these problems remain challenging, because a compiler throws away valuable information during compilation from source to binary code.

A different approach

For many tasks, complete decompilation may not be required. Given a binary blob, one may be satisfied by knowing which parts are in the program. To this end, it is sufficient to compare all binary sequences of the program with a database containing known, benign sequences. If a sequence of the currently analyzed program matches one in the database, then we can easily identify the original component, such as its source code or its version.

In December 2023, for example, Ghidra – the NSA's disassembling framework – added such a component to aid binary identification.

Our research in this area started in 2021 and addresses the problem in a lasting, novel way. First, to drive this research, we need to produce a large database of known, good binary code. To this end, we create a compilation farm that can compile large amounts of programs with different compilers, and their different versions. Since the resulting binaries require enormous quantities of space, we *hash* the binaries using a variety of different hashing techniques.

Second, once we analyze a new program, we hash the program with the same set of different hashing techniques and look up these hashes in our database containing the precomputed hash data. If we find a match, we have a high confidence that the binary sequence in question is benign and we have seen it before. Consequently, there is no need to actually analyze the sequence. Since we can perform such a lookup on all sequences of a program, we can essentially filter out all known sequences, allowing manual reverse engineering efforts to focus on the unknown sequences instead. Thus, available resources can be used in a more optimal fashion, leading to better overall results.

👤 Prof. Dr. Stefan Brunthaler

@ brunthaler@unibw.de

☎ +49 89 6004 7330

🌐 www.unibw.de/ucsrl-en

Prof. Dr. Michaela Geierhos

Data Science

The interdisciplinary team of the Professorship of Data Science combines expertise from the fields of computer science, computational linguistics, and mathematics 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 to support decision-making processes. It uses methods and insights from fields such as mathematics, statistics, stochastics, 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). The type of data is very diverse: in addition to text, audio signals and images are also processed.

In particular, this includes the development of algorithms for (semantic) text analysis, which has practical applications in social media mining, which in turn can be used to detect threats to objects of protection or to identify disinformation campaigns. The detection of deep fakes using innovative Artificial Intelligence (AI) methods is also part of the range of applications. As data synthesis is often misused for disinformation, fraud and other malicious purposes, the detection of synthetic image data needs to be more reliable in the future.

Practice-oriented training

The 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.

Practice-oriented research: Data science use cases

Research also combines theory and practice. The Data Science team has numerous collaborations with partners in the military, corporate, and public sector. Current applications range from the detection of disinformation campaigns and the reconstruction of audio data to the use of trustworthy AI in police applications. One goal of the current research is the prototypical implementation of a single framework capable of decoding differently coded audio signals. A particular focus is on speech reconstruction. AI techniques, in particular Generative Adversarial Networks, will be used for this purpose.

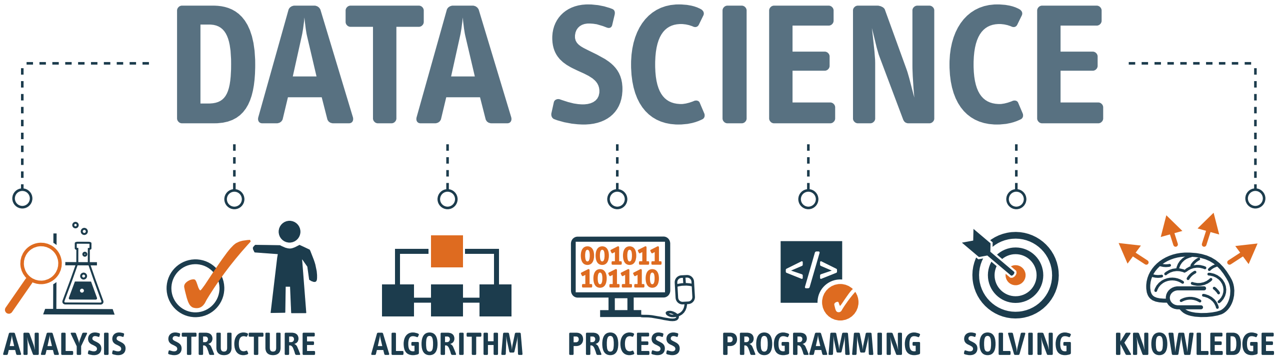
Recent technological advances and developments in AI are enabling its application in many areas. However, the question about trustworthiness continues to arise. For the transparent use of trustworthy AI models for text classification by security authorities, we want to ensure that they can be explained. Law enforcement agencies need to analyze a wide variety of text forms in large volumes, so AI methods can provide crucial support in identifying suspicious content with high speed and accuracy. However, the decisions made by an AI model are not easy to explain. Our goal is therefore to develop solutions that provide understandable explanations for different police scenarios in order to build confidence in the decisions.

Prof. Dr. Michaela Geierhos

@ michaela.geierhos@unibw.de

☎ +49 89 6004 7340

www.unibw.de/datascience



Range of tasks covered by the Professorship of Data Science.

FIG.: SHUTTERSTOCK / RYZHI; SHUTTERSTOCK / TRUEFFELPIX

Project SynData

Generation and detection of synthesized visual data

Due to recent breakthroughs in Deep Learning, applications driven by Artificial Intelligence enable users to generate synthesized images and videos within a few button clicks. This causes difficulties in estimating the authenticity of the information, and synthesized data with malicious intent can have profound implications. This motivates the project SynData, which deals with the generation and detection of synthesized visual data.

What are image and video synthesis?

Artificial intelligence (AI) processes images, text, and other data types in specifically designed numerical representations. Upon processing, the model is then required to perform a specific task, which historically has been simple tasks like regression (numerical prediction) or classification of inputs.

Nowadays, models can be used for tasks that are much more complex, like automated robotics or data generation. The latter requires complex network structures, carefully curated datasets, and days of training to produce strong generators.

Once trained, however, these models can create visual data that looks authentic (e.g., realistic portraits of faces), even with prerequisites predefined by the user that directly affect the synthesized scene.

What is synthesis detection and why is it relevant?

Synthesis based on AI has been improved to a point where anyone with no prior knowledge of Deep Learning can create deceivingly real text, images, and even videos within a few button clicks. Therefore, the design and improvement of detection algorithms that numerically predict if data is real or synthesized is currently a trending research topic.

Current design choices for image generators often result in specific artifacts that are present in every synthesized image. These flaws in the architecture of generators can be exploited to design detectors that are trained to find those artifacts in images. Detectors are usually very deep neural nets that have been pretrained exhaustively on large-scale databases and are then finetuned to detect generation artifacts in specific datasets.

AI-generated images: Artificial intelligence enables the manipulation of facial features in the generation process.

What is SynData?

The project SynData is separated into two teams where each team focuses on either synthesis or detection. Both have built experimentation frameworks that allow for the testing of state-of-the-art (SOTA) models and the building of new architectures for specific use cases. The generation team works on providing better data synthesis that is of higher quality and less detectable. The detection team aims to build fast and robust detection algorithms that reliably classify images as “synthesized” or “real”. The topical separation into synthesis and detection allows for constant interaction and improvement on both sides, as an improvement for one team presents a new challenge for the other team. As part of the project, the teams have already drafted, formulated, and experimented with novel approaches to both feature selection in image synthesis and adversarial attacks to evaluate the robustness of SOTA detectors. Some of those novelties were published at high-ranking conferences or are currently in the final stages of evaluation.

Amon Soares de Souza, M.Sc.

amon.soares@unibw.de

+49 89 6004 7342

https://go.unibw.de/syndata

FIG.: ZITIS / A. MEISSNER

Project NAWI

News Articles and Knowledge

The NAWI project is dedicated to the extraction of structured knowledge from Cyber Threat Intelligence (CTI) reports using Relation Extraction, Named Entity Recognition, and Entity Linking methods. The resulting knowledge will transfer into a graph that can be used for temporal analysis and the prediction of correlations based on pre-existing knowledge in the cybersecurity domain.

Threat of cyber attacks and the role of CTI reports

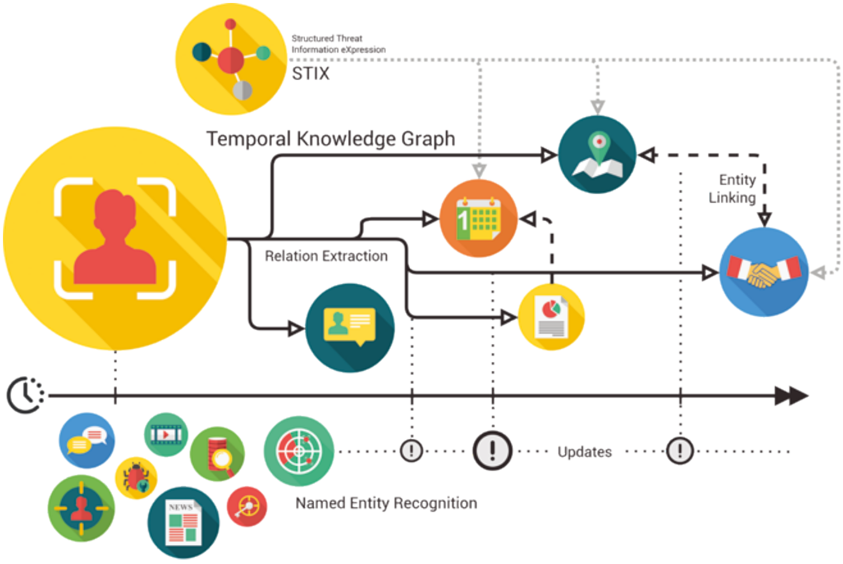
Today's interconnected world is constantly facing the threat of cyber attacks, which not only cause financial damage but also threaten the integrity of sensitive data and the continuity of processes. In context, CTI reports play a crucial role.

They provide deep insights into the tactics, techniques and procedures (TTPs) used by attackers, as well as the latest threats and vulnerabilities. As a result, CTI reports provide an information-rich resource for automated extraction of information.

Improved preparation through evaluation of CTI reports

In particular, the information contained in CTI reports about past attacks helps to better prepare for future attacks. By analyzing and structuring this data, valuable information about different incidents and actors can be identified to better respond in future attacks. To address this problem, the project focuses on generating a knowledge graph from CTI reports.

With the help of advanced semantic analysis techniques such as Relation Extraction and Named Entity Recognition, the project aims to capture the actors, tools, methods, and the like in the reports and to show their interrelationships.



Techniques utilized to generate temporal knowledge graphs structured in STIX format.

Semantic analysis of CTI reports

From daily generated CTI reports, relevant information will be converted into the STIX serialization format, which describes the inherent textual relationships. For this purpose, the ontology provided by STIX is used. Named Entity Recognition is used to identify entities in the text, while at the same time, the corresponding relation is predicted using Relation Extraction.

Knowledge graph in cyber security

After the extraction of semantic information, the identified entities have to be linked to the knowledge graph using Entity Linking, which is continuously updated. Another focus of the research is the criteria that must be fulfilled in order for new information to be integrated into the graph. In a later step, Link Prediction enables the prediction of missing or future information. In addition, the project can automatically extend existing knowledge graphs.

Florian Babl, M.Sc.

florian.babl@unibw.de

+49 89 6004 7352

https://go.unibw.de/nawi

FIG.: RI CODE / F. BABL

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 as well as their practical application under the motto "Development and operation of secure networked applications."

THE TEAM OF the Professorship of Software and Data Security pursues the goal of developing solutions for real-world-relevant security challenges under the consideration of operational boundary conditions, that are typically part of the operation of complex IT infrastructures.

Research and projects with third parties therefore usually begin with a comprehensive empirical analysis, in which, for example, relevant components from the designated application area are either cloned into virtual environments or at least their core characteristics are modeled and simulated to facilitate detailed analysis. This approach allows, among other things, the explorative application of offensive test procedures and thus the qualitative and quantitative analysis of vulnerabilities in complex multi-step attack scenarios. From this, security requirements can be systematically derived, which serve as a basis for the subsequent constructive activities and a later practical evaluation of the results achieved.

The design of new and improved IT security measures follows the security engineering approach: On the one hand, they are designed, modeled, and simulated on a technical level, and on the other hand, they are integrated as seamlessly as possible into the design, implementation, and operational processes of the intended application areas, also from an organizational perspective. An essential requirement is the concrete implementation with subsequent evaluation, which takes place at a minimum in the laboratory but, if possible, also in concrete pilot environments and ideally by individual embedding in scientifically accompanied projects. The role of the human factor in information security, economic, and legal constraints is also taken into account.

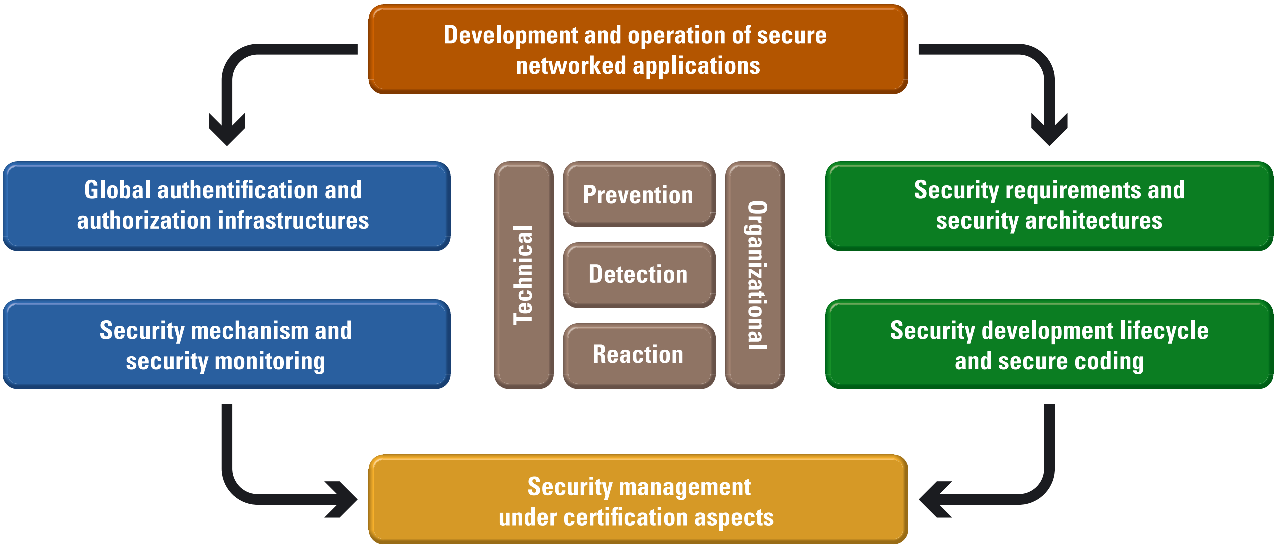
In 2023, ongoing research and projects included work on linking decentralized identity management solutions with user-friendly and data protection-optimized approaches to document signatures. Innovative approaches to securing communication protocols, security monitoring and policy-driven automation solutions were applied to the management of future energy supply networks. The adaptation of Security Information & Event Management (SIEM) systems to low-latency requirements and new types of threats is the subject of a project to analyze and secure 6G mobile networks. The transfer of research results into practice has also been achieved within the framework of dtec.bw projects: For example, the first components of a flash flood early warning system were put into operation as part of a cooperation with the district of Bad Kissingen. The key data for a secure crisis communication infrastructure based on commercial-off-the-shelf IoT components was defined in collaboration with the municipality of Neuhaus and disaster control and emergency services.

Prof. Dr. Wolfgang Hommel

@ wolfgang.hommel@unibw.de

☎ +49 89 6004 7355

www.unibw.de/software-security


Development and operation of secure networked applications
Global authentification and authorization infrastructures
Security mechanism and security monitoring
Technical
Prevention
Detection
Reaction
Organizational
Security requirements and security architectures
Security development lifecycle and secure coding
Security management under certification aspects

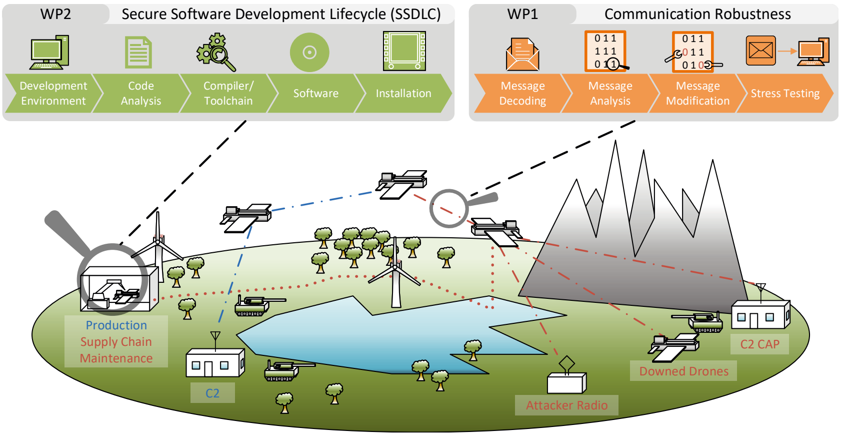
Main research topics of the Professorship of Software and Data Security.

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

Project ACSE

Airborne Cybersecurity Enhancement

The Airborne Cybersecurity Enhancement (ACSE) project is a research collaboration between FI CODE and Airbus Defence and Space (Airbus). Our team is involved with network security for internal and external communication of aircraft on one hand and secure software development in avionics on the other and is in close contact with current Airbus projects.



Considered attack vectors for aerial vehicles in ACSE.

Security in communication networks

The goal of the subproject is to create an opportunity to analyze network protocols used in avionics with regard to potential vulnerabilities and to prototype new protocols.

To this end, a comprehensive analysis of various internal and external communication protocols currently in use was first carried out, with communication protocols from other domains that could potentially be used in aviation also being included. The protocols were evaluated according to a standardized system and areas of application and potential weaknesses were identified. Based on this general classification, parts of specific avionics architectures were then considered and proposals for hardening them were developed.

Using this knowledge and a review of the state of the art for analyzing and interacting with protocols on all ISO-OSI levels for wired and wireless communication, a tool was then developed that allows interaction with various interfaces in order to test them. The main focus was on reducing the initial effort for the integration of new protocols by utilizing the protocol specifications already available internally at Airbus. Thanks to the flexibility achieved, the tool is also suitable for prototyping protocol changes or completely new protocols.

Security in software development

This subproject investigated how the development process of software for avionics systems can be adapted to take cyber security into account in addition to the already existing extensive standards and requirements of the aerospace industry.

On the conceptual side, a “Secure Software Development Life Cycle” (SSDLC) was developed, which incorporates the existing requirements, primarily due to operational safety, as well as the current development processes at Airbus and expands them with modules to increase cyber security.

One specific component for increasing cyber security is the use of software analysis tools. This subproject examined how certain programming languages and programming rules used in aerospace can be checked with such tools and which categories of errors and associated vulnerabilities can be avoided.

Alexander Frank

+49 89 6004 2745

alexander.frank@unibw.de

https://go.unibw.de/acse

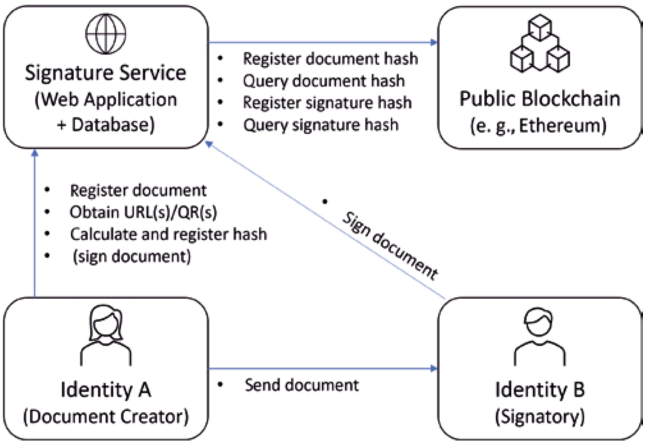
Funded by:
Airbus Defence and Space

FIG.: RI CODE / ALEXANDER FRANK

Project LIONS

Ledger Innovation and Operation Network for Sovereignty

The LIONS project is building a research platform to increase resilience and digital sovereignty in digitalization using distributed ledger technologies. As part of the transdisciplinary research project, the research group is focusing on the topics of self-sovereign identity management, electronic signatures, and technical support for the project partners.



LIONS architecture for digital signature services.

DIGITAL IDENTITIES are a central component of increasingly digitalized everyday life. In this context, the work package in the LIONS research project contributes to considering not only technical aspects of identity management systems, but also the link to topics from psychology and human-machine interaction.

Self-sovereign identity management

As a contribution to greater transparency and data protection in the handling of personal data, self-sovereign identity management involves users centrally in the management of their identity data.

This creates both technical challenges in adequately securing this data and organizational hurdles in the exchange and acceptance of identity data. In addition, questions are investigated that analyze how users interact with the identity wallets.

The technical advantages of the system are contrasted with the almost complete transfer of responsibility for the secure use of identity data to the users.

Electronic signatures

In the context of identity management, digital signatures play a decisive role as cryptographic proof of identity. At the same time, together with the identities themselves, they form the basis for electronic signatures, which are an indispensable component of digitized business processes.

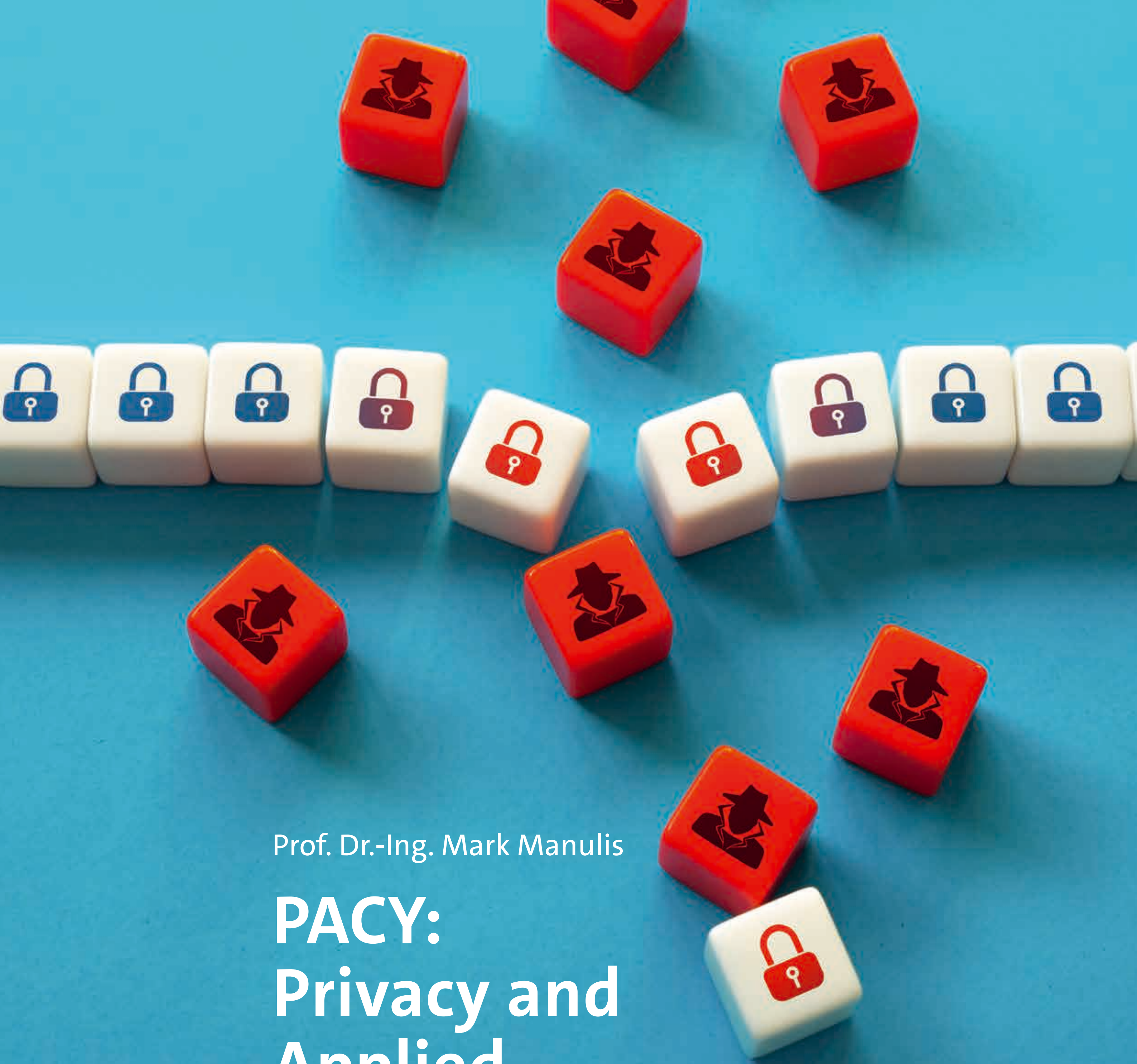
As part of the project, various concepts for exchanging signed data and documents are being developed, prototyped and demonstrated. For this purpose, the direct exchange of data between two identities or their mobile devices was examined by modifying a standardized data format using scenarios from the healthcare and military-organizational fields. The applications and libraries required were implemented, tested for both scenarios and presented at conferences.

Furthermore, a concept for a web- and Ethereum-based system for electronic signatures was developed and prototypically implemented, which focuses primarily on aspects such as usability, trustworthiness, data protection and increased sovereignty. In this system, the public blockchain is used to make the data verifiable without coming into conflict with data protection. New methods for placing signatures on the document are also being evaluated. In this context, an empirical study has also been prepared to examine existing and new concepts for trustworthiness and acceptance.

Dr. Michael Grabatin
michael.grabatin@unibw.de
+49 89 6004 3992
https://www.unibw.de/lions

Funded by:
dtec.bw
Funded by
the European Union
NextGenerationEU

FIG.: RI CODE / MICHAEL HOFMEIER



Prof. Dr.-Ing. Mark Manulis

PACY: Privacy and Applied Cryptography Lab

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 foci at the PACY Lab

PACY Lab was established in March 2022 and is part of the RI CODE. Its research staff have 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.

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 modeling and an 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. 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.

Privacy and Applied Cryptography Lab

PACY

Analysis Design • Engineering

In the design and implementation of new PEC approaches, 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. 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. 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, 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

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

ARKG: Asynchronous Remote Key Generation

Encapsulating cryptographic key pairs for public-key cryptosystems

Asynchronous Remote Key Generation (ARKG), introduced by PACY Lab in collaboration with Yubico in 2020, was initially designed to enable backup of security keys for web accounts protected by the WebAuthn/FIDO2 standard. Since then, ARKG has proved itself as a standalone building block for other applications in delegated and privacy-preserving authentication.

Difference between ARKG and standard key encapsulation mechanisms

In traditional key encapsulation mechanisms (KEM) the sender uses the public key of the receiver to encapsulate a symmetric cryptographic key K. The intended receiver can decapsulate K using its own private key. One of the main uses of KEMs today is in the establishment of secure channels where the encapsulated key K is used to derive further symmetric keys to protect the communication between the involved users.

FIG.: GENERATED BY DALL-E 3

In contrast, ARKG allows the sender to encapsulate the entire asymmetric key pair (sk, pk) for the intended receiver such that only the receiver (and not the sender) learns the private key sk. This essentially allows the receiver to later use (sk, pk) as its own freshly generated key pair in public key cryptosystems. Since its introduction in 2020, ARKG has proved itself to be a versatile building block enabling a range of different applications in the context of delegated or delayed authentication.

ARKG for pairing-based and post-quantum-secure cryptosystems

In 2023, PACY Lab continued to work on new ARKG designs. The original version of the ARKG protocol from 2020 was designed for discrete logarithm-based key pairs and hence could only be used in relevant cryptosystems such as ECDSA signatures or ElGamal encryption. The new constructions of ARKG published by PACY Lab in 2023 have significantly expanded the scope of applications for ARKG towards other types of key pairs that are commonly used in modern cryptography.

Our first result published at ACNS 2023 is a general ARKG approach for generating key pairs that are compatible with many pairing-based cryptosystems. For example, instances of our pairing-based ARKG protocol can generate keys compatible with special-purpose digital signature schemes such as schemes by Pointcheval and Sanders from 2016 or Camenisch and Lysyanskaya from 2004 that are used in anonymous credential systems.

Another instance of the protocol can be used to generate keys for stealth addresses that are based on BLS signatures and can be used to provide receiver-anonymity in blockchain transactions.

Our second result published in IEEE EuroS&P 2023 is a quantum-safe ARKG protocol which can be used to generate key pairs that are compatible with a range of lattice-based cryptosystems, including a Kyber key encapsulation mechanism and Dilithium signature, which were chosen by NIST as future standards in post-quantum cryptography.

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

Fast and Expressive Searchable Encryption

Enabling expressive search queries over outsourced encrypted data.

Searchable encryption allows users to outsource confidential data to a cloud storage in an encrypted form and later perform private search operations without trusting the cloud provider with the confidentiality of their data.

Challenges when searching over encrypted data

Outsourcing data storage to third-party providers offers an efficient way for clients with limited resources or expertise to manage and disseminate large volumes of encrypted data. However, traditional public or private key encryption methods capable of protecting data confidentiality at rest hinder the ability to selectively search and retrieve specific data segments.

The emerging cryptographic concept of Searchable Encryption (SE) aims to address these limitations. SE allows users to securely outsource data (e.g., files, databases) to a cloud storage in an encrypted form and later perform search operations on their data without disclosing the searched contents to the cloud provider. As such, SE can be seen as part of the emerging paradigm behind confidential computing or computing over encrypted data where cloud services need not be trusted with data confidentiality or private-key management.

Expressive searchable encryption from attribute-based encryption techniques

In the design of modern SE approaches based on public key cryptography, the so-called key-policy attributed-based encryption (KP-ABE) is an important building block. In a KP-ABE scheme, each private (decryption) key has an embedded access policy and can be used to decrypt ciphertexts that in turn embed attributes for which the access policy is satisfied. For example, a ciphertext containing attributes Officer and Army can be decrypted by a private key with embedded suitable access policies such as Officer OR Army or Officer AND Army. KP-ABE can be used to construct an SE scheme by viewing attributes embedded into ciphertexts as keywords that can be used by search queries, whereas the search queries can be viewed as access policies embedded into private keys. In order to enable encrypted search keywords will be embedded into the ciphertexts at the time of encryption, whereas appropriate private keys are generated on-demand based on required search queries. In order to ensure that keywords remain confidential, a special flavor of so-called anonymous KP-ABE schemes must be used as a building block.

FIG.: GENERATED BY DALL-E 3

PACY Lab is working on efficient public key-based SE schemes that are capable of handling expressive search queries where contained keywords can be represented via conjunctive, disjunctive, or any monotonic Boolean formulae to enable practical use in real-world applications. To this end, in collaboration with the University of Surrey (UK), we designed and implemented the most efficient anonymous KP-ABE scheme and showed how to turn it into a fast and expressive SE scheme called FEASE. The resulting SE scheme achieves better performance and scalability when compared to the state-of-the-art public key-based SE schemes. This work will appear in Usenix Security 2024.

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

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

The Artificial Intelligence & Machine Learning (AIML) research group, led by Prof. Eirini Ntoutsi, focuses on developing intelligent algorithms to address data-related societal challenges. Ongoing research directions include a) continuous learning and unlearning, b) responsible AI focusing on fairness, explainability and robustness, and c) generative AI for improving data quality.

Continuous learning

Numerous applications, including communication networks, social media, and production processes, generate dynamic data that continuously arrives in the form of streams. The dynamic nature of data streams requires a shift from traditional training routines to continual learning, where models adapt to and evolve continuously with incoming data. The focus of Artificial Intelligence & Machine Learning (AIML) is on developing intelligent algorithms that learn continuously from evolving data, while considering resource and performance constraints on memory and response time, for example.. The research addresses updating ML models with new data, managing historical information to prevent catastrophic forgetting, adapting to evolving features, and monitoring and explaining changes over time. This research direction is exemplified by projects such as OSCAR, concentrating on textual streams, and HEPHAESTUS, which focuses on manufacturing data streams.

Responsible AI

AI-based systems are widely employed nowadays to make decisions that have far-reaching impacts, hence entailing concerns about potential human rights issues. To ensure the responsible development and deployment of such systems for the benefit of the society, it is essential to move beyond traditional algorithms optimized solely for predictive performance and integrate ethical and legal principles into the design, training, and deployment of AI systems. Research focus is addressing bias and discrimination in AI systems, explainable AI (XAI), and robustness. In fairness-aware learning, multi-fairness and challenges such as class imbalance are explored. In XAI, the group studies counterfactual explanations and uncertainty modeling, while in robustness, the goal is to enhance model generalization and strengthen them against adversarial attacks. This research direction is exemplified by projects such as NoBIAS and MAMMoth which focus on fairness, and STELAR, which focuses on robustness to bias sources.

Generative AI

AI is no longer limited to analyzing historical data; it can now generate new content, spanning text, images, and tabular data. Generative AI holds potential for societal benefits, aiding engineers in product design, inspiring new creations, and contributing to content generation. However, challenges including security issues, biased content, copyright concerns, and creative limits must be addressed. The AIML group leverages generative AI to address data quality challenges, including imbalances and biases. Additionally, its potential in generating new data and solutions beyond the limitations of existing datasets is explored. This research direction is illustrated by projects such as SFB1463, focusing on the design of next-generation offshore wind turbines through a combination of simulation, analytical, and data-driven models.

Development of the Research Group

In 2023, the group expanded with the addition of six Ph.D. students and 1 postdoc, while some members remain in Berlin (at the Freie Universität) and Hannover (at the Leibniz University/L3S Research Centers), where Prof. Ntoutsi was previously affiliated.

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

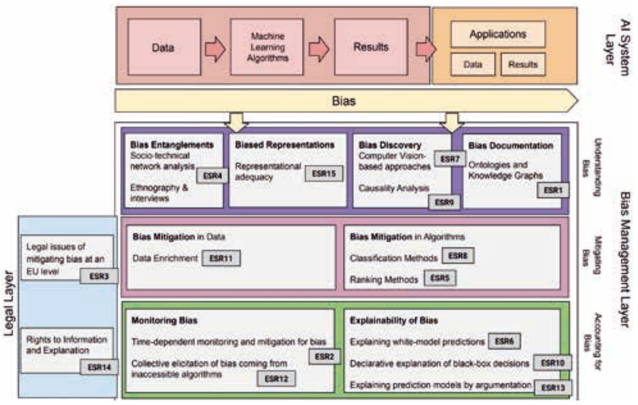
https://www.unibw.de/aiml-en

FIG.: ADOBE STOCK / PARRADEE; ADOBE STOCK / THITICHAYA

Project NoBIAS

Artificial Intelligence without BIAS

In NoBIAS, we conduct research and develop innovative methods for bias-aware AI-decision making. The project aims to deliver a cohort of 15 researchers trained to identify biased and discriminating AI decision making and able to provide solutions that reconcile and fully exploit AI while ensuring compliance with legal and social norms.


Data
Machine Learning Algorithms
Results
Applications
Data
Results
AI System Layer
Bias
Bias Entanglements
Socio-technical network analysis
ESR4
Ethnography & interviews
Biased Representations
Representational adequacy
ESR15
Bias Discovery
Computer Vision-based approaches
ESR7
Causality Analysis
ESR9
Bias Documentation
Ontologies and Knowledge Graphs
ESR1
Understanding Bias
Bias Mitigation in Data
Data Enrichment
ESR11
Bias Mitigation in Algorithms
Classification Methods
ESR8
Ranking Methods
ESR5
Mitigating Bias
Monitoring Bias
Time-dependent monitoring and mitigation for bias
ESR2
Collective elicitation of bias coming from inaccessible algorithms
ESR12
Explainability of Bias
Explaining white-model predictions
ESR6
Declarative explanation of black-box decisions
ESR10
Explaining prediction models by argumentation
ESR13
Accounting for Bias
Bias Management Layer
Legal Layer
Legal issues of mitigating bias at an EU level
ESR3
Rights to Information and Explanation
ESR14

NoBIAS research agenda overview.

AI: Unlocking potential while mitigating risks

Artificial Intelligence (AI) algorithms are extensively employed by businesses, governments, and various organizations to make decisions with far-reaching impacts on individuals and society. While these algorithms provide solutions to diverse problems, they also pose risks, potentially resulting in discriminatory outcomes such as job denials or unequal medical treatments. The observed discriminative impact on specific population groups in various cases has raised concerns about the societal implications of the technology.

Addressing these concerns is crucial to ensure that AI technology contributes to social good while harnessing its significant potential. Responsible development and deployment of AI play a crucial role in ensuring ethical use, fostering trust, and ensuring accountability in implementing these powerful technologies.

Holistic approach to tackling bias in AI systems

In NoBIAS, the primary focus is on addressing bias and discrimination in AI systems, adopting a holistic approach that encompasses the entire AI decision-making pipeline. The overarching goal is to understand the various sources of bias, detect them as they manifest, and mitigate their effects on the produced results for specific applications. Achieving this goal is made possible through an interdisciplinary approach combining computer science, law and sociology and a coordinated set of individual projects that share a global vision towards bias-aware AI systems.

Main objectives:

1. Understanding the creation of bias in society, its entry into sociotechnical systems, its manifestation in the data used by AI algorithms, and how it can be modeled and formally defined.
2. Developing methods and techniques to mitigate bias at various stages of AI decision-making, including data, algorithms, and models.
3. Utilizing proactive methods like bias-aware data collection and retroactive approaches such as explaining AI decisions in human terms (XAI) to address bias in outcomes.

The interdisciplinary NoBIAS consortium consists of eight organizations, including a non-academic one, spread across five European states with leading expertise in AI, law and sociology. The network is complemented with various associated non-academic partners from different application domains including banks and health care.

NÔBIAS

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

https://nobias-project.eu/

Funded by:
European Union's Horizon 2020 research and innovation programme under the **Marie Skłodowska-Curie** grant agreement No. 860630.

FIG.: RI CODE / NTOUTSI

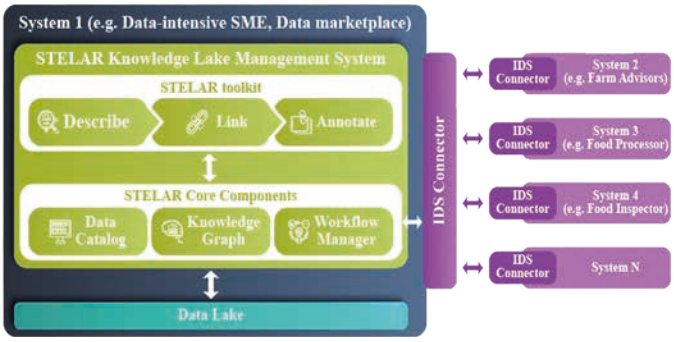
Project STELAR

Spatio-TEmporal Linked data tools for the AgRifood data space

STELAR develops an innovative Knowledge Lake Management System (KLMS) to boost FAIR (Findable, Accessible, Interoperable, Reusable) and AI-enhanced (high-quality, reliably labeled, bias-aware) data practices in the agrifood sector, one of nine key data areas in the European Data Strategy. Pilots cover risk prevention in food supply, early crop growth prediction and timely precision farming interventions.

AI in agriculture

AI is revolutionizing agriculture, enhancing efficiency, precision, and decision-making, ushering in a significant shift in the sector and paving the way for a more sustainable and productive future. Despite these advancements, navigating the complexity of the agrifood domain presents challenges, including integrating diverse data sources, addressing biases and data quality issues, managing the substantial volume of data produced through sensors, satellites and other sources and coping with the enormous variety of downstream tasks and applications.



An overview of STELAR KLMS.

In STELAR, the group focuses on developing a Knowledge Lake Management System (KLMS) for the agrifood data space that enables intelligent discovery, semantic interoperability, and provides AI-ready data, supporting applications in smart agriculture and food safety.

Main objectives:

1. Optimize data discovery and reuse by automating the extraction of detailed metadata, including domain-specific indicators and summaries, to enhance energy-efficient analytics on large data volumes.
2. Improve data linking and interoperability with linked data technologies for enriched descriptions, interlinked entities, and addressing schema- and instance-level matching, spatio-temporal data alignment, and correlations.
3. Improve data annotation and synthetic data generation using advanced learning techniques and mechanisms for explainability, bias detection and mitigation, addressing label and data scarcity.

The KLMS will be pilot tested on real-world agrifood use cases, namely risk prevention in food supply, early crop growth prediction and timely precision farming interventions.

This group's primary focus is to enhance data quality for various AI-based downstream tasks, facilitating model generalization across diverse contexts (space, time, weather, crop types etc) and independent of data biases. This begins with analyzing AI pipelines to identify sources of bias and understand their effect on downstream task models. Following this analysis, generative AI can be leveraged to enhance data quality and employ explainable AI (XAI) for inspection, ensuring that the models learn accurate information.

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

Dr. Vivek Kumar

vivek.kumar@unibw.de

https://stelar-project.eu/

Funded by:
EU as part of the call for proposals HORIZON-CL4-2021-DATA-01-03 – Technologies for data management (IA)

FIG.: STELAR PROJECT

Prof. Dr. Daniel Slamanig

Cryptology

The Quantum Safe & Advanced Cryptography (QuSAC) Lab, headed by Prof. Dr. Daniel Slamanig, is conducting research into provably secure quantum-resistant public-key cryptography and advanced cryptographic primitives. Our research is motivated by the growing security requirements due to the increasing pervasive connectedness and rapid technological development.

THE QUSAC LAB, led by Prof. Dr. Daniel Slamanig, holder of the Professorship of Cryptology, conducts research in foundations and applications of cryptography. Our primary focus is on quantum-resistant public-key cryptography and advanced cryptographic primitives. We consider both modular constructions based on generic cryptographic building blocks as well as ones based on concrete mathematical assumptions. In doing so, provable security plays a central role in our work.

Relevance of cryptography

Cryptography is at the core of cyber security. It improves security and privacy of most modern digital services and applications and is highly relevant to society. However, the complexity of modern scenarios also places high demands on the security and functionality of cryptography.

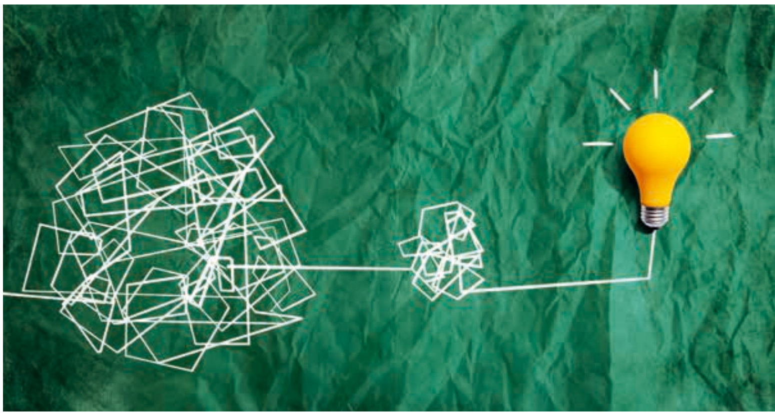
Stronger security properties – quantum computers and more

Potential advances in the field of quantum computing would make the currently used public-key cryptography insecure. This risk can be mitigated by relying on quantum-resistant (or post-quantum) cryptography. We conduct research on classes of mathematical problems underlying the construction of quantum-resistant schemes (e.g., isogeny-based cryptography) as well as on the design of (advanced) cryptographic primitives. Notably, Prof. Slamanig was involved in the design of the Picnic post-quantum digital signature scheme. It was submitted to what is arguably the most important international post-quantum cryptography standardization project from NIST and there reached the final third round.

Aside from this significant challenge imposed by the quantum threat, some desirable or required security guarantees for modern scenarios are often not provided by basic cryptographic primitives either. Here, for example, we are working on the development of public-key encryption primitives that provide the required strong security properties, as well as on the theoretical foundations of privacy-preserving cryptography.

More functionality and stronger security

Modern applications are increasingly complex and require advanced functionality while at the same time providing high security guarantees. This requires cryptographic mechanisms whose functionality goes far beyond basic primitives. Here, for example, we conduct research on non-interactive zero-knowledge proofs and their succinct variants (so-called SNARKs), which nowadays represent the most widely used advanced cryptographic concept in the real world.



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

Contributions to the academic community

In 2023, Prof. Slamanig was invited to serve on the program committees of various top-tier conferences: 44th Annual International Cryptology Conference (CRYPTO 2024), 31st Annual ACM Conference on Computer and Communications Security (ACM CCS 2024), 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2023), and the 30th Annual ACM Conference on Computer and Communications Security (ACM CCS 2023). At ACM CCS 2023 he received a Top Reviewer Award, which honors the top 10% most constructive reviewers among the program committee.

Development of the Research Group

The QuSAC Lab has been established in November 2023 and the first two Ph.D. students started in December. From February 2024, the lab additionally hosts a postdoc. The group has a strong national and international scientific network and maintains numerous collaborations. Joint future projects are already being planned and will further contribute to the growth of the QuSAC Lab.

👤 Prof. Dr. Daniel Slamanig

@ daniel.slamanig@unibw.de

☎ +49 89 6004 7430

🌐 www.unibw.de/crypto-en

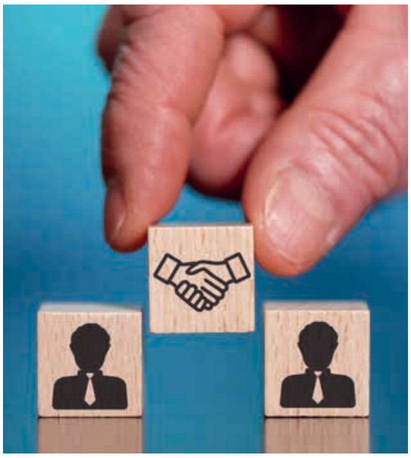
FIG.: ADOBE STOCK / ANNIKA; ADOBE STOCK / TIERNEY

Fine-Grained Forward Security via Puncturable Encryption

How to let cryptographic keys “forget” how to decrypt certain ciphertexts?

Encryption is a fundamental cryptographic mechanism but can only provide security if the secret keys are kept secret. Considering that secure management of cryptographic keys is a notoriously hard task, it is too idealized to assume that they will never leak. Since sensitive information often need to be protected for a long time, certain applications can benefit from encryption schemes with stronger security properties.

WE HAVE WELL-STUDIED formal frameworks to rigorously define what it means for encryption schemes to be secure. Using methods from provable security, we can then mathematically prove that encryption schemes satisfy a certain notion of security.



Modern applications put encryption solutions to the test.

FIG.: ADOBE STOCK / THODONAL

Encryption and key leakage

Encryption schemes, however, only provide security if the secret keys are not known to an adversary. Nowadays, encrypted data are exchanged over public networks and often stored on third party servers (e.g., the cloud). Storage space is cheap and thus one needs to assume that data will exist in storage for a long time (e.g., in backups) or will even be intentionally recorded while in transit and stored for later use, as suggested by the Snowden leaks. Considering that the secure management of cryptographic keys is a notoriously hard task, it seems far too optimistic to assume that secret keys will never leak. Especially, when taking into account that sensitive information often must be protected for several decades.

Protecting data into the future

The formal property capturing the protection of encrypted data produced prior to leaking a secret key is called forward security. This property is well understood for interactive key-exchange protocols and mandatory in major secure communication protocols like TLS 1.3. However, as soon as one removes interaction, the picture changes. This is for instance the case in public-key encryption or low-latency key-exchange protocols that have zero round-trip time (0-RTT), i.e., where encrypted data can already be sent in the first message of the sender.

Key puncturing

Such a property is provided by encryption schemes which allow puncturing the secret key in a very fine-grained way, i.e., on ciphertexts. Here, a key that has been punctured on a certain ciphertext is then not able to decrypt this ciphertext anymore. Consequently, even if this punctured key leaks, the message protected by the respective ciphertext is not in danger. Members of the QuSAC Lab have proposed the first efficient puncturable encryption (PE) scheme (called Bloom Filter Encryption), various algorithmic optimizations for concrete schemes, a generic way to construct such schemes from post-quantum assumptions as well as various generalizations of PE schemes. Worth mentioning here is viewing another primitive called updatable encryption, an approach to rotate keys for outsourced encrypted data without requiring downloading and re-encrypting all the data, from a puncturable perspective. This enables the construction of such schemes with strong forward security guarantees. Despite significant progress in recent years, there are still many interesting open questions related to PE.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

Strengthening Non-Interactive Zero-Knowledge Proofs

Making non-interactive zero-knowledge proofs ready for the real-world

Zero-knowledge proofs (ZKPs) are a fascinating concept. They allow a party (the prover) to interactively convince another party (the verifier) of the validity of a statement without revealing any information beyond this fact: for example, proving that you have solved a Sudoku puzzle without revealing its solution. In recent years we have seen a "Cambrian explosion" in research and practical deployment, the latter posing numerous challenges.

ZKPS HAVE BEEN invented in the mid-1980s and non-interactive zero-knowledge (NIZK) proofs are an interesting variant. Here, the proof is a single message from the prover and can be verified by anyone. This feature, however, comes at the cost of requiring an all-trusted entity to set up some common information available to all parties.

Growing interest in zero-knowledge proofs

For a long time, the concept was mainly of theoretical interest and real-world use has been limited. With the growing popularity of cryptocurrencies and blockchains, this picture has drastically changed. For real-world applications there is a particular interest in NIZK with succinct proofs, so-called zk-SNARKs.

Two crucial security properties of NIZK proofs

The zero-knowledge property requires that proofs do not leak any information about the so-called witness, which the prover requires to convince the verifier of its claim. The soundness property ensures that a verifier will not accept proofs for false claims. For the latter, one typically requires the stronger knowledge soundness property, meaning that the prover indeed needs to know the witness, instead of only showing its existence. However, when NIZKs are used in the wild, not even this is sufficient, and one requires so-called simulation extractability (SE). Loosely speaking, this guarantees that proofs cannot be "mauled", i.e., it is not possible to obtain a different valid proof from observing some valid proof(s). This is important for cryptocurrency applications, as otherwise an adversary could generate new coins out of thin air. Another interesting application are signature schemes, where members of the QuSAC Lab have demonstrated how to construct quantum-safe signatures from certain SE NIZKs.

Proving knowledge of puzzle solutions without revealing them.

FIG.: ADOBE STOCK / THODONAL

Proving the SE property, however, is a tedious task. Members of the QuSAC Lab have introduced generic compilers that allow to "lift" NIZK proofs or zk-SNARKs that are just (knowledge-) sound to SE ones without affecting the efficiency too much. The latter is particularly important for zk-SNARKs, where succinctness and efficiency play an important role.

The all-trusted entity in the real-world

If the initial setup process is performed maliciously, then the security of the NIZK breaks down. While in theory one can simply assume an honest setup, in many real-world settings there typically does not exist a party trusted by everyone. One important research direction is the design of NIZK proofs that provide security even if the setup is subverted. This is a very active field of research and members of the QuSAC Lab have extensively contributed to this field. However, many interesting open questions remain.

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

Prof. Dr. Arno Wacker

Privacy and Compliance

Don’t just teach data privacy and compliance, live it!

ONE OF OUR MOST important goals 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 way. We also want to show the general public that technologies that promote data protection can be integrated into everyday life, both in the private and business spheres.

Teaching

In the professorship, teaching is divided into pentesting, data protection, privacy-enhancing technologies, 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 tried and tested best practice documentation. Cryptology teaches the basics 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 to support privacy and data protection and is divided into three different research areas:

- Privacy-supporting mechanisms aim at strengthening the privacy of individuals as well as researching communication rules for the Internet age.

- Increasing IT security awareness is concerned, among other things, with the area of self-data protection. To this end, the professorship develops and researches methods and tools to increase security awareness in the development of software tools and in their use.

- The cryptanalysis of classical ciphers investigates the field of classical encryption methods with the help of modern (meta-)heuristic methods. Among other things, the efficiency of the analyses and the security of the algorithms are examined.

Knowledge transfer

A particular concern of our professorship is to train, educate, and inform interested members of the public about IT security issues. We pursue this goal with lectures and workshops on topics such as pentesting, secure email traffic in everyday life 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; ISTOCK / PESHKOV

The CrypTool Project

Open source software for learning cryptography and cryptanalysis

The CrypTool project (www.cryptool.org) is a collection of software applications, teaching and learning material on the subject of cryptography. It focuses on historical methods as well as applications that are used in modern IT environments. Since March 2023, the overall project management has been at the Chair of Data Protection and Compliance of Prof. Wacker.

CRYPTOOL (CT) is primarily used in university teaching, but is also used by students, amateur cryptologists and historians. The Decrypt project https://de-crypt.org, for example, is currently working on a software pipeline to enable the automated decryption of old archive finds. CrypTool software components are part of this pipeline. The crypto challenge website MysteryTwister www.mysterytwister.org, which is based at the University of Bochum, is also linked to the project.

CT was originally launched in 1998 by Prof Esslinger (University of Siegen) as an awareness tool during his time at Deutsche Bank. Under his leadership and with the help of numerous volunteers, students, researchers and challenge solvers from all over the world, the project has continued to develop ever since. The technical infrastructure had already been relocated to Prof Wacker's Chair of Data Protection and Compliance in Munich in 2019, and this year the main project responsibility was finally transferred to him. Dr Behrendt has been responsible for the further development and maintenance of the CT project as project manager since March 2023.

In addition to several smaller sub-projects, our work in 2023 focused on two main areas:

1) The first focus was on converting the web application CrypTool-Online (CTO, https://www.cryptool.org/de/cto/) to the "mobile first" paradigm using modern web technologies. CTO contains around 50 cryptography apps, e.g. an AES animation, Msieve factorization or Caesar encryption. Each of these apps must be ported from the current infrastructure, based on a Jekyll rebuild of the original CrypTool portal, which was built with Joomla, to the new infrastructure. The new infrastructure uses Next.js, React and Chakra UI, among others.

Students have the opportunity to port one of the CTO apps as part of their Bachelor's or Master's thesis at Mr Wacker's professorship and receive support from experienced full-stack web developers from the CT project. The initial work is already underway.

The transition to the new CTO should be successfully completed in 2024.

2) The second focus is on implementing newer methods into CTO, particularly in the areas of post-quantum cryptography and fully homomorphic encryption. The first prototypes have been built here, although it has become clear that more mathematical foundations are needed to understand them.

The development of such basic apps is another goal for 2024.

Prof. Dr. Arno Wacker

@ arno.wacker@unibw.de

☎ +49 89 6004 7325

www.unibw.de/datcom

FIG.: RI CODE / A. WACKER

Detection of Cookie Banners

Recognition, recording and evaluation of cookie banners

This dissertation project investigates the automated recording and analysis of cookie banners on websites. The aim is to develop the most accurate method possible for identifying and evaluating cookie banners. The project is intended to provide a comprehensive overview of compliance with guidelines regarding cookie banners on websites. These guidelines result from the General Data Protection Regulation (GDPR).

THE PROJECT will analyze different techniques and approaches to determine the most effective method for detecting and classifying cookie banners. The classification of cookie banners is based on whether a cookie banner is manipulative or not. This categorization helps us to assess whether a cookie banner meets the requirements of the GDPR or not. Among other things, the options offered by the cookie banner (reject/accept) and their color design are used as criteria for this classification. The setting of cookies by the website is also relevant, as not only must the banner be correctly designed, but third-party cookies may only be set in the background after the user has given their consent.

The manual process for evaluating cookie banners is precise, but slow and time-consuming. An evaluation based on fixed terms or structures in the HTML code is also out of the question. Due to the variety and flexibility with which cookie banners can be displayed, e.g., through positioning, different wording and embedding of the banners on the website, this procedure is not an option. Therefore, the focus is on machine learning (ML) and investigating how ML can be used to automatically recognize and classify cookie banners and, if necessary, extract relevant information from them. This includes the development and training of models, the testing of various methods and their optimization.

Initial approaches using ML to recognise whether a cookie banner is present or not have shown an accuracy of 70 to 90 percent, depending on the approach.

The linguistic formulation of the text is also relevant for classification, as a banner must be easy for the user to understand in accordance with the GDPR. This still poses a major challenge for ML approaches. A model would have to be trained that can judge whether a given text for a cookie banner is easy for a person to understand or not.

All these steps – recognizing a banner, classifying it into different ways of manipulating the user – will build on each other. It is therefore unlikely that it will be possible to develop a single model that performs all these steps in one go.

As a result of the project, a statement is to be made about the distribution of websites on the Internet with regard to cookie banners, whether they inform the user correctly and also behave correctly when cookies are set or not.

Mathias Schlolaut, M.Sc.
mathias.schlolaut@unibw.de
+49 89 6004 7328
www.unibw.de/datcom

FIG.: ISTOCK / WONGMBATULOYO

Prof. Dr. Gabi Dreo Rodosek

Communication Systems and Network Security

The professorship deals with the use of generative AI/ML in network security and social media analytics, software-defined networking, 5G/6G networks, detection, assessment and mitigation of cyber risks.

Project CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

CONCORDIA was one of the pilot projects to build a European secure, resilient and trusted ecosystem with leading research, technology, industrial and public competences. It has combined excellence and leadership to overcome fragmentation by building the ecosystem to strengthen European digital sovereignty.

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

MORE THAN 21 highlights, over 300 scientific publications, a multi-stakeholder ecosystem bringing together research, industry, start-ups, and public bodies: All this and more has been achieved by CONCORDIA, which ended on March 31, 2023. The four-year, €16-million project (plus €7 million in additional industrial funding) covered a wide range of topics, including cyberattacks on critical infrastructure, information security and data protection, certification, and competence building. CONCORDIA has fully achieved its objective of building a European resilient, secured, and trusted ecosystem, being agile, innovative, and open. Furthermore, CONCORDIA's results will not only provide valuable input to the European Cybersecurity Competence Centre and the network of National Cybersecurity Centres, and with this to the whole European cybersecurity community, but will also strengthen and speed up research, development, and innovation. CONCORDIA was also mentioned in the BMBF yearbook "Success Stories 2023".

One of CONCORDIA's highlights is the proposed Roadmap for Cybersecurity in Europe, a set of strategic recommendations and priorities concerning research and innovation, education, economics and investment, law, certification, and standardization. The CONCORDIA Service Board was specified to allow to build and manage the cybersecurity community. The KYPO Cyber Range Platform addresses the education and training of cybersecurity professionals, developed by Masaryk University, and released as open source in 2020. The KYPO Cyber Range received the 2021 EU Innovation Radar award in the Disruptive Tech category. Defence against DDoS attacks is addressed by the DDoS Clearing House, successfully piloted in Italy and the Netherlands. Sharing data and the experience of experts about attacks helps organizations find out what attacks exist so they can prepare for them in advance. Developing CONCORDIA's Cyber Threat Intelligence Platforms for the telco and finance sectors, including a legal framework ("Code of Engagement") and security metrics, are further project achievements. CONCORDIA's initiative Women in Cybersecurity implemented actions to incentivize gender diversity. The CONCORDIA's Governance Model for a European Education Ecosystem in cyber security was specified based upon the experiences gained from CONCORDIA's course Becoming a Cybersecurity Consultant, whose successful attendees were able to apply for the C3, CONCORDIA established certification scheme for the cybersecurity consultant role. These initiatives, including the Teach-the-Teacher activity, addressed the lack of cybersecurity professionals by providing training and certification of cybersecurity skills. A Framework for Risk Analysis, the CONCORDIA Insurace Model and the Ecosystem of Startups are other examples of project achievements.

The CONCORDIA consortium started with 42 partners, funded by the EU. At the end of the project the CONCORDIA consortium consisted of 56 project partners, from academia, industry, and public bodies, representing 21 EU member states and Horizon 2020 associated countries with partners contributing own resources to the project objectives.

Prof. Dr. Gabi Dreo Rodosek
@ gabi.dreo@unibw.de
☎ +49 89 6004 7360
https://www.concordia-h2020.eu/

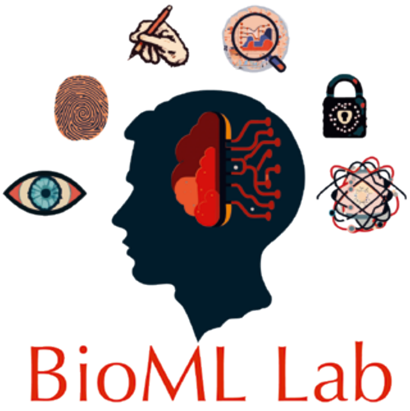
Funded by:
The European Union's
Horizon 2020 research
and innovation program
under grant agreement
No. 830927.

FIG.: ADOBE STOCK / DENIS PUTILOV; CONCORDIA CONSORTIUM

Prof. Dr. Marta Gomez-Barrero

BioML: 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 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 standardization 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, 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.

Biometrics & cryptography

The main issue with biometric recognition, in contrast with passwords, is the fact that we cannot revoke our fingerprint or our face and issue a substitute characteristic. Thus, we need tools to protect these sensitive data. Applying common cryptographic algorithms like hashes or RSA is however not the solution we are looking for: Every time we acquire a biometric sample we include noise, which would lead to incorrect results for operations carried out on encrypted data.

Therefore, BioML researches how to apply homomorphic encryption techniques or other forms of irreversible transformations (e.g., Bloom filters) to biometric data in order to protect the privacy of the subjects in an end-to-end manner.

Detecting biometric presentation attacks

As any other security technology, biometric systems are subject to external attacks. The simplest form of attack, not requiring any technical knowledge from the attacker, involves presenting a fake biometric characteristic (e.g., a silicone face mask or a thin fingerprint overlay) to the capture device in order to fool the system.

This is known as a presentation attack, which has been a very active area of research in the last decade. Given that we cannot predict which new forms of presentation attacks will appear in the future, BioML develops detection methods based on traditional two-class classifiers as well as on anomaly detection techniques.

Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml-en

FIG.: ISTOCK / DILOK KLAISATAPORN; RI CODE / MARTA GOMEZ-BARRERO

Prof. Dr. Udo Helmbrecht

Quantum Communication

Within the framework of dtec.bw project MuQuaNet is constructing a quantum network in the Munich metropolitan area in cooperation with partners in academia and industry. The goal is to establish test and research operations of a quantum communication network with selected civil and military applications.

MuQuaNet

Pioneering quantum-secure communication in Munich

In a world where digital security is becoming increasingly important, the MuQuaNet project is setting new standards in the field of quantum-secure communication infrastructure. Aiming to demonstrate Quantum Key Distribution (QKD) for both civilian and military applications, the project is making significant strides towards network integration in the greater Munich area.

Testing diverse QKD systems

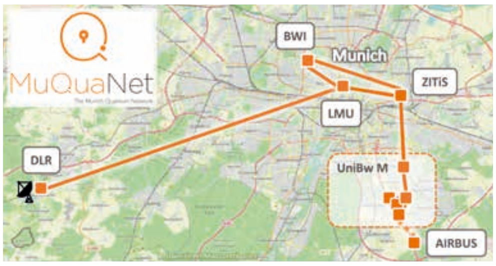
MuQuaNet integrates various Quantum Key Distribution (QKD) systems from multiple manufacturers. These different devices are tested in real-world scenarios to better understand the efficiency of QKD in multiple contexts:

- *LMU Free-Space System:* This QKD system, developed in collaboration with LMU, is based on the BB84 protocol. It focuses on miniaturization and examining atmospheric disturbances.
- *ID Quantique:* Their systems use either the Coherent One-Way (COW) protocol for simplicity or a Time-Bin BB84 protocol for enhanced security.
- *Quantum Optics Jena:* These systems are based on entanglement, offering the highest security through quantum randomness and the non-clonability of quantum states.
- *QuantLR:* Israeli systems, similar to ID Quantique, using the Time-Bin BB84 protocol but with specific optimizations, especially in cost.

Combining these diverse systems aims to create a robust infrastructure for quantum-secure communication in the greater Munich area.

Key management as the core

Challenges arise in the interoperability of different QKD systems due to the need for standards. Therefore, a focus is on key management to distribute quantum keys securely. One aspect involves trusted relays, which are necessary for transmitting keys over long distances but require trust in the intermediate nodes and do not offer absolute security. Hence, reinforcement through additional mechanisms is essential.



MuQuaNet fiber-optic network.

Local KMS with Rohde & Schwarz

A local Key Management System (KMS) has been developed to integrate QKD into SITLine encryptors by Rohde & Schwarz. These encryptors are suitable for critical environments and meet the requirements for VS-NfD approval at OSI Layer 2. Future developments will include hybridization with other key exchange methods and managing complex network infrastructures.

MKR with TU Ilmenau and secunet

An alternative approach has been developed for SINA VPNs to meet the VS-NfD approval requirements at OSI Layer 3. These use Multi-Path Key Reinforcement (MKR), which combines key material from independent paths to enhance security. This is particularly advantageous for the robustness of key distribution in complex networks. MuQuaNet significantly contributes to developing quantum-secure communication for authorities and critical infrastructures. Combining various approaches enhances the protection of data, with important implications for Munich and Europe.

👤 Hon.-Prof. Dr. Udo Helmbrecht
@ udo.helmbrecht@unibw.de
👤 Dr. Nils gentschen Felde
@ felde@unibw.de
☎ +49 89 6004 7375
🌐 www.unibw.de/muquanet

Funded by:
dtec.bw
Funded by the European Union
NextGenerationEU

FIG.: TAUSENDBLAUWERK.DE / M. KRÄMER; RI CODE / MUQUANET / F. FARINA

Jun. Prof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

Jun. Prof. 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.

Project AI-GDP

AI-based guidance development processes: Innovative decision-making in health care

This project specifies and identifies the role that Artificial Intelligence (AI) can play in public health-related intelligence analysis, decision-making, and especially guidance development processes (GDP). AI technologies have established a benchmark in a variety of management areas. Thus, they can be a great ally in the achievement of the World Health Organization's mission in future normative guidance development processes.

Artificial intelligence in public health intelligence analysis and guidance development

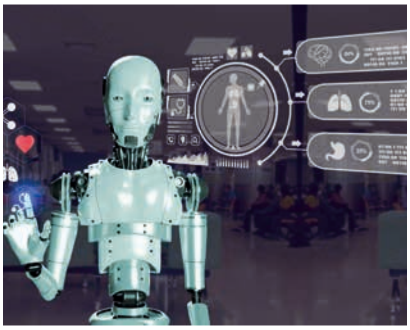
Public health intelligence analysis can be widely benefited from AI, particularly by facilitating real-time surveillance and predictive modeling. It can also improve foresight capabilities (i.e., for epidemic and pandemics, crises), monitor health trends, and evaluate the effectiveness of health interventions and guidelines.

Guidance development and quality assurance of fast-track normative products

The project characterizes how AI can facilitate the automation of data collection, particularly when dealing with vast amounts of information, real-time data, and data produced in different languages and formats (e.g., written, image, or audios). There is a particular focus on integrating data from diverse set of sources (e.g., electronic records, guidelines, social media, etc.) and thus on facilitating a comprehensive real-time data gathering. Some innovative examples include AI-controlled searching processes, AI-enabled wearables, and AI-driven drones,

Key AI technologies that may influence guideline development processes

Among others, AI can facilitate the analysis of large amounts of data in a quicker and more accurate way. This can reflect the most recent updates in data and trends, standardize processes to facilitate replicability and consistency, and reduce human error.



Optimization of public health intelligence reporting

The project and related workshops demonstrated that AI can contribute to tailoring public health intelligence reports to different target audiences, facilitating the decision-making process. Among others, the tailoring process can be done according to the following variables: language translation (retaining meaning in a target language), diverse expertise (adjusting complexity and technical terms), and formats (text, presentation, infographic, audio-visual content).

Artificial intelligence in public health decision-making: An innovative living approach

AI-enabled decision-making systems in the public health sector can offer significant advances, such as in the development of normative guidelines, allocation of resources, diagnostics and treatment planning, among others, to support a future living approach. Examples of these systems include expert systems (emulating human decision-making based on expert knowledge), prescriptive analytics (forecasting consequences to optimize the decision process), and consensus algorithms (aggregation of opinions).

Prof. Dr. Maximilian Moll

Prof. Dr. Stefan Pickl

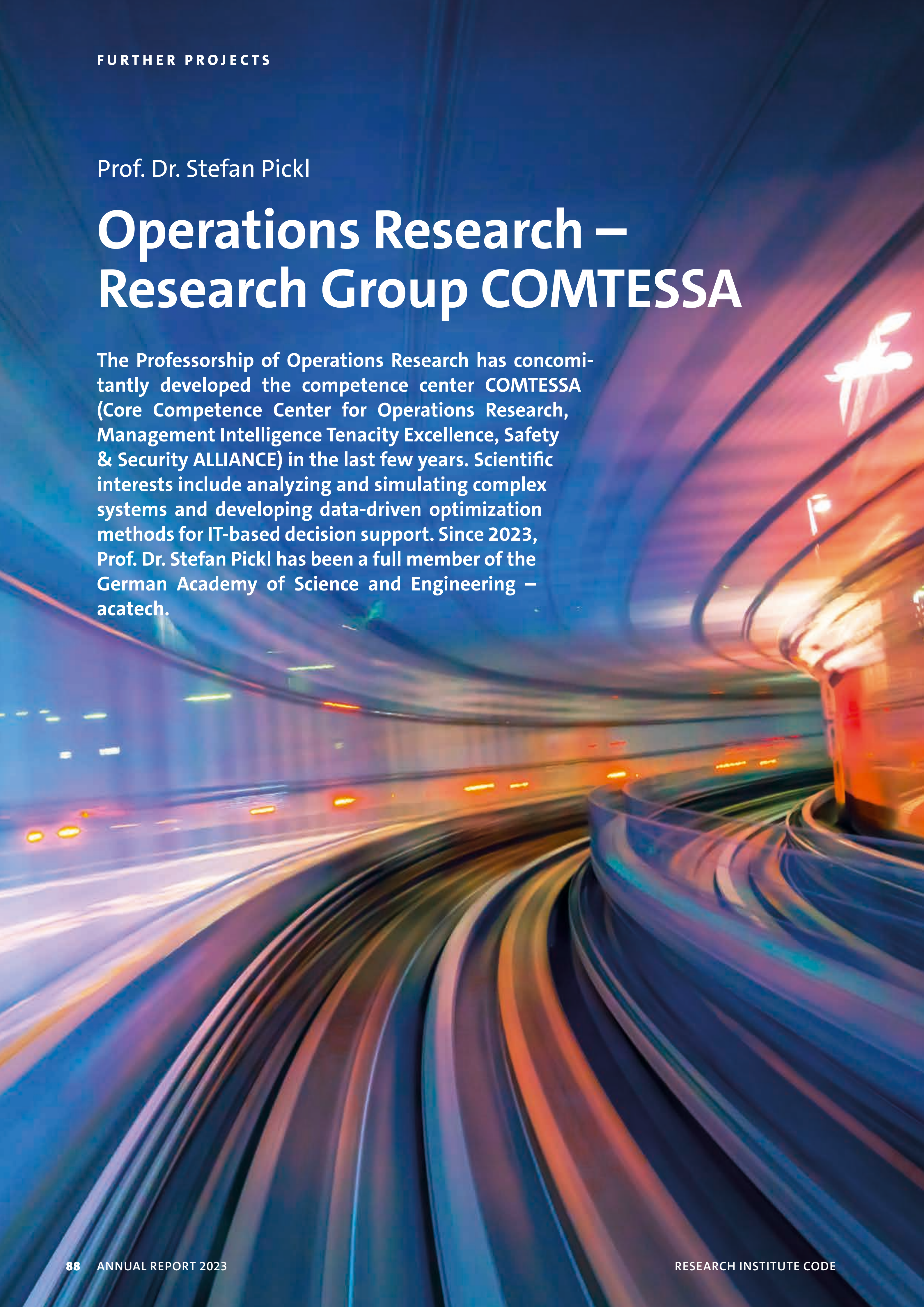
@ stefan.pickl@unibw.de

☎ +49 89 6004 2400

https://go.unibw.de/aigdp

Funded by:
WHO

FIG.: ADOBE STOCK / TIERNEY; ADOBOE STOCK / APITHANA



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.

Project 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.

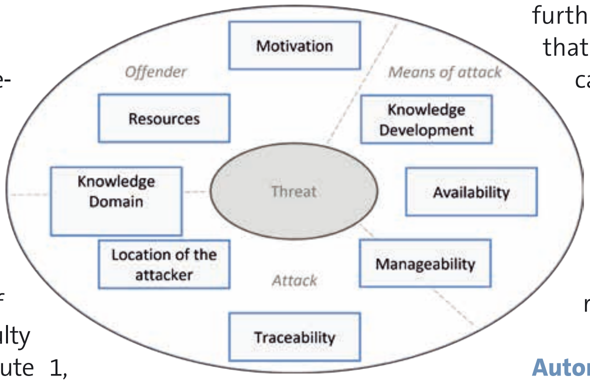
Objective

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, Faculty of Computer Science – Institute 1, Chair for Operations Research, the COMTESSA research group (project management) in cooperation with the CODE research center, as well as IVE Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH), CreaLab GmbH, and the TU Braunschweig, Institute of Transport, Railway Construction and Operation (IVE).

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. After extensive research, more than 500 physical and almost 1000 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.

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.

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

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

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

PD Dr. Corinna Schmitt

National Coordination Center for Cybersecurity

RI CODE is a partner of the National Coordination Center for Cybersecurity (NCC-DE) for Germany for military cybersecurity research in close cooperation with the BMVg. The aim of this initiative by the European Commission is to establish national coordination centers of excellence that monitor research and development in the field of cyber security, to establish a national network for the exchange of knowledge, and to identify new research directions and aspects for the European Commission's agenda and programs.

THE EUROPEAN PARLIAMENT and the European Council have agreed to establish the European Cyber Security Centre (ECCC) and a network of national coordination centers across the European Union based on EU Regulation 2021/887. The ECCC and the network are intended to pool investments in research, technology, and industrial development in the field of cyber security and to better coordinate the planning of the Horizon Europe and Digital Europe programs.

In Germany, the National Coordination Center (NCC-DE) for Cybersecurity in Industry, Technology and Research is a joint effort of

- the Federal Ministry of Defense (BMVg) and the affiliated research institute Code with a focus on military cyber security research,
- the Federal Ministry of the Interior and Homeland (BMI) with a focus on all aspects of cyber security,
- the Federal Ministry of Economics and Climate Protection (BMWK) with a focus on supporting industry, SMEs, and start-ups,
- the Federal Ministry of Education and Research (BMBF) with a focus on research in civil security, and
- the DLR Project Management Agency in close cooperation with the BMBF and BMWK.

The BSI acts as the central point of contact for the ECCC, the NCC network and the national players.

The NCC-network will intensify the exchange between the member states and enable interested parties from administration, industry and research in the EU to find partners for multilateral projects more quickly and easily, thereby strengthening the EU's digital sovereignty. Within the individual member states, the respective NCC promotes and intensifies the dialog and exchange between interested national partners. In this way, the flow of information to the ECCC is consolidated to optimally support the national cybersecurity community and ensure that national interests are effectively represented in the EU funding process.

The core tasks of the NCC-DE are to network the national cybersecurity community, support the cybersecurity community in participating in EU funding programs, develop contributions to EU funding programs "Horizon Europe" and "Digital Europe", and continuously collect and exchange information at national and European level, including in the special committees. To accelerate the development of the NCC-DE and enable the rapid implementation of the core tasks in the start-up phase, part of the consortium raised additional funding as part of the "Digital Europe" program at the end of 2023. At the same time, these are also used to gain an insight into the current research situation and an overview of urgent and pressing research needs to connect partners or pass on topics to the ECCC for the future agenda.

NCC-DE Team at the CODE Annual Conference 2023 (f. l. t. r.): Stefan Hillesheim (DLR-PT), Dr. Marvin Richter (DLR-PT), PD Dr. Corinna Schmitt, Dr. Alexander Khanin (DLR-PT), Heiko Siebel (BSI), Christian Sick (BSI).

PD Dr. Corinna Schmitt

corinna.schmitt@unibw.de

☎ +49 89 6004 7314

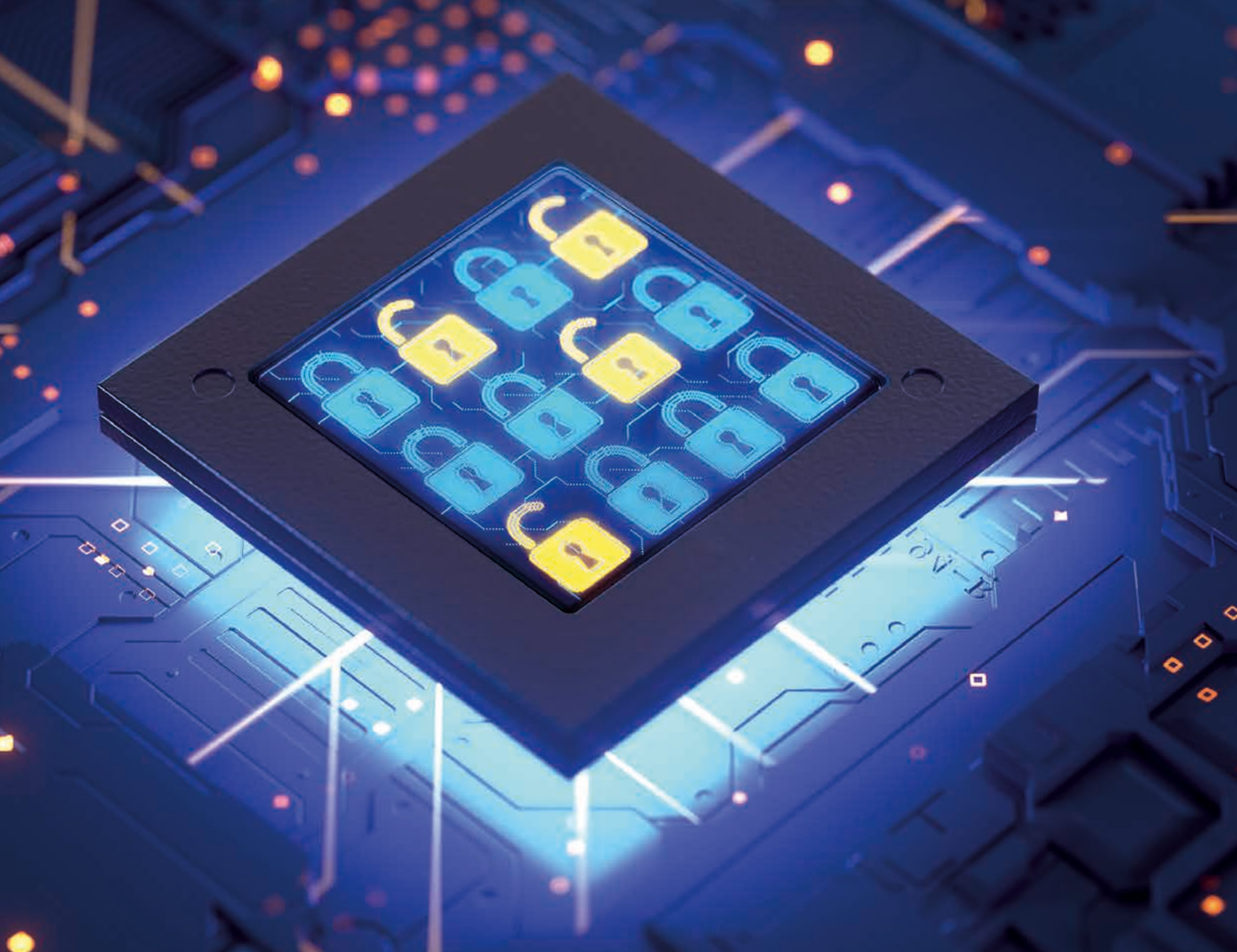
https://nkcs.bund.de

Funded by:
The European Cybersecurity Competence Centre
under Grant Agreement No. 101126787

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

FIG.: ADOBE STOCK / YOUR 123; RI CODE / CORINNA SCHMITT

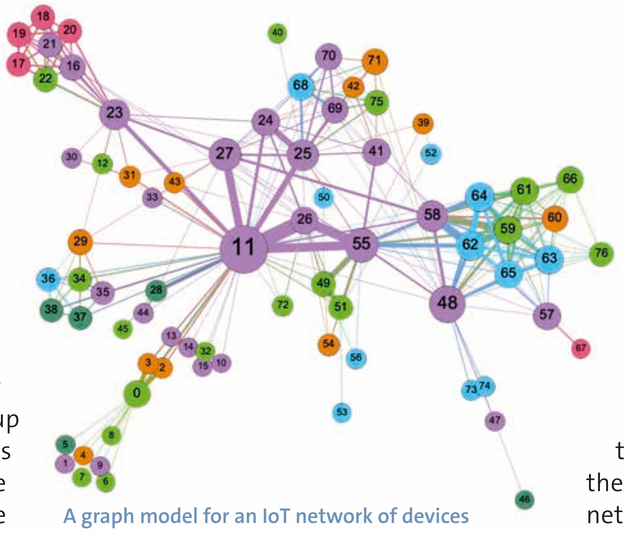


Prof. Dr. Gunnar Teege

Formal Methods for Securing Things (FOMSET)

The research group FOMSET applies formal methods to achieve IT security in the domain of embedded and cyber-physical systems. This involves methods such as the formal software verification of operating systems and graph-theoretical modeling of IoT networks. The research is conducted in PhD projects and in cooperation with industry partners.

THE GOAL OF the research group of Prof. Dr. Gunnar Teege is to increase the use of formal methods for securing IT systems. The group examines different kinds of systems and studies the methods which are applicable to achieve specific security properties for them.



A graph model for an IoT network of devices with different properties.

Formal verification of system software

System software, such as device drivers and other operating systems components, is often crucial for the security of the complete IT system based on it. Therefore, the formal confirmation that it does not contain errors or vulnerabilities is of high relevance for the whole system. At the same time system software is still implemented today in programming languages such as C or C++ or even assembly languages, which makes the application of formal verification methods difficult and expensive.

The goal of the working group is to increase the degree of automatization for formal proofs about system software supported by mathematical proof assistants like Isabelle or Coq.

Attesting cloud systems based on microkernels

Users of a cloud system must be able to rely on the system to protect security properties for their applications, such as integrity and confidentiality with respect to other users. This requires that the cloud system does not allow violations of these properties and that it can prove this to the user by transmitting manipulation-safe evidence about it (“attestation”). The research in the group investigates the realization of such evidence based on microkernels, such as the formal verified seL4 kernel.

Graph-based modeling of malware infections in IoT networks

The huge number and often weak security facilities of the single devices in IoT (Internet of Things) networks mostly prevents the application of conventional measures, such as security software updates, for securing such networks against attacks. The research in the group investigates graph-based models of the devices and their connections to identify security relevant structures in the networks and to exploit them against attacks. For this purpose, it transfers methods to IoT networks which have been developed and applied for information propagation in social networks and also for the spreading of infectious diseases.

Securing vehicular networks using blockchain technology

Interconnected vehicles exchange information among each other and with the traffic infrastructure. This exchange is most effective if as many instances participate in it as possible. At the same time, a large number of participants increases the risk of attacks on integrity, availability, and possibly confidentiality of the information. Blockchain technology has been developed for cryptocurrencies and is also applied for the tracking of goods. For its application in vehicular networks it must be modified and adapted. The research in the group investigates necessary modifications which make blockchain technology applicable to achieve verifiable security properties for vehicular networks.

Prof. Dr. Gunnar Teege

gunnar.teege@unibw.de

Phone: +49 89 6004 3353

Web: www.unibw.de/fomset

FIG.: [M] SHUTTERSTOCK / BLUE ANDY, ISTOCK / MATEJMO; FARELL FOLLY

FIG.: ADOBE STOCK / GREENBUTTERFLY

Cooperations

Germany and the World

National Partners

The RI CODE is working with 96 partners in 47 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.

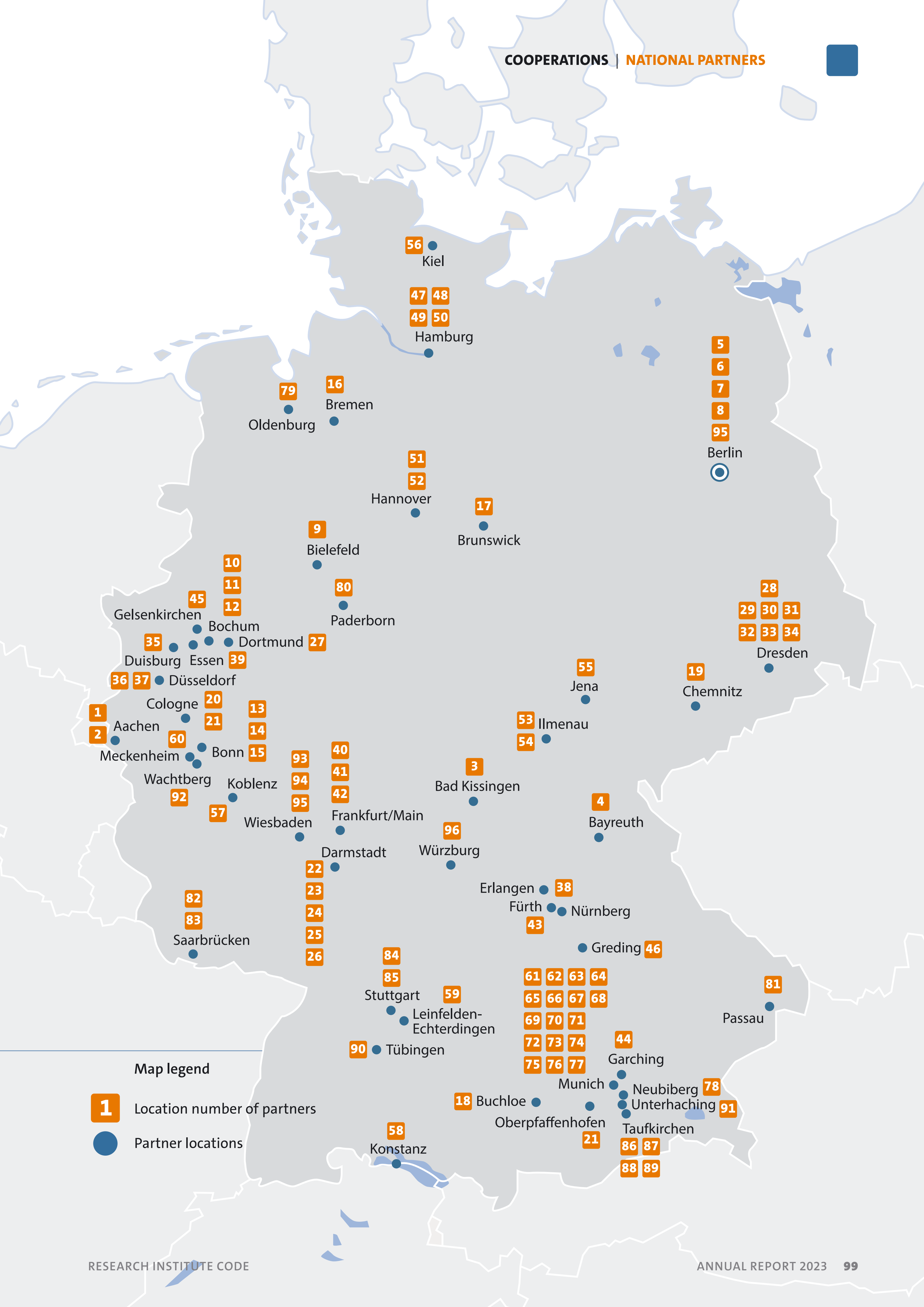
Within Germany, our network is particularly tight-knit. As part of the University of the Bundeswehr Munich, we work with 96 institutions in 47 cities and municipalties nationwide. The focus is on Bavaria and the Munich area, North Rhine-Westphalia, and Hessia. ■

	Partner	Location
1	RWTH Aachen University	Aachen
2	Utimaco Management Services GmbH	Aachen
3	District of Bad Kissingen	Bad Kissingen
4	University of Bayreuth	Bayreuth
5	Akhetonics GmbH	Berlin
6	DIN	Berlin
7	HWR Berlin	Berlin
8	Deutsches Forschungsnetz (DFN)	Berlin
9	Bielefeld University of Applied Sciences and Arts (HSBI)	Bielefeld
10	IDEMIA Identity & Security Germany AG	Bochum
11	Max Planck Institute for Security and Privacy	Bochum
12	Ruhr University Bochum (RUB)	Bochum
13	Federal Office for Information Security (BSI)	Bonn
14	ZDigBw	Bonn
15	DLR-PT	Bonn
16	Constructor University gGmbH	Bremen
17	Technical University of Braunschweig	Brunswick
18	f.u.n.k.e. AVIONICS GmbH	Buchloe
19	Chemnitz University of Technology	Chemnitz
20	SoSafe GmbH	Cologne
21	German Aerospace Center (DLR)	Cologne/Oberpfaffenhofen
22	Fraunhofer Institute for Computer Graphics Research (IGD)	Darmstadt
23	GSI Helmholtz Centre for Heavy Ion Research	Darmstadt
24	Darmstadt University of Applied Sciences (h_da)	Darmstadt
25	National Research Center for Applied Cybersecurity ATHENE	Darmstadt
26	Technical University of Darmstadt	Darmstadt
27	RapidMiner GmbH	Dortmund
28	HZDR	Dresden
29	TU Dresden	Dresden
30	CampusGenius GmbH	Dresden
31	Meshmerize GmbH	Dresden
32	Wandelbots GmbH	Dresden
33	Mimetik UG	Dresden
34	Enari GmbH	Dresden
35	University of Duisburg-Essen (UDE)	Duisburg/Essen
36	State Criminal Police Office NRW (LKA NRW)	Düsseldorf
37	Rheinmetall AG	Düsseldorf
38	Friedrich-Alexander University of Erlangen-Nuremberg (FAU)	Erlangen/Nuremberg
39	secunet Security Networks AG	Essen
40	Frankfurt University of Applied Sciences	Frankfurt a. M.
41	nuix	Frankfurt a. M.
42	Droniq GmbH	Frankfurt a. M.
43	KEEQuant GmbH	Fürth
44	Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities (LRZ)	Garching
45	AWARE7 GmbH	Gelsenkirchen
46	WTD 81	Greding
47	Bundeswehr Command and Staff College (FüAkBw)	Hamburg
48	Helmut Schmidt University/University of the Bundeswehr Hamburg (HSU/UniBw H)	Hamburg

FIG.: ADOBE STOCK / KRAS99 / TAUSENDBLAUWERK.DE

	Partner	Location
49	DFN-CERT Services GmbH	Hamburg
50	Hamburg University of Technology (TUHH)	Hamburg
51	Leibniz University Hannover (LUH)	Hanover
52	Hannover Medical School	Hanover
53	Fraunhofer Institute for Digital Media Technology (IDMT)	Ilmenau
54	Technical University Ilmenau	Ilmenau
55	Quantum Optics Jena GmbH	Jena
56	Christian-Albrecht University of Kiel (CAU)	Kiel
57	Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw)	Koblenz
58	University of Konstanz	Konstanz
59	Minol-ZENNER-Gruppe	Leinfelden-Echterdingen
60	BWI GmbH	Meckenheim
61	Center for Digital Technology and Management (CDTM)	Munich
62	ESG Elektroniksystem- und Logistik-GmbH	Munich
63	FAST-DETECT GmbH	Munich
64	fortiss GmbH - Research Institute of the Free State of Bavaria for software-intensive systems	Munich
65	Google Munich	Munich
66	Hanns Seidel Foundation	Munich
67	LMU Munich	Munich
68	Munich Police Department	Munich
69	Rohde & Schwarz GmbH & Co. KG	Munich
70	Siemens Energy AG	Munich
71	Technical University of Munich (TUM)	Munich
72	VISTA Remote Sensing in Geosciences GmbH	Munich
73	Central Office for Information Technology in the Security Sector (ZITiS)	Munich
74	Siemens AG	Munich
75	BMW AG	Munich
76	Olive Robotics GmbH	Munich
77	Cadami GmbH	Munich
78	Infineon Technologies AG	Neubiberg
79	University of Oldenburg	Oldenburg
80	Paderborn University (UPB)	Paderborn
81	University of Passau	Passau
82	CISPA Helmholtz Center for Information Security	Saarbrücken
83	INM – Leibniz Institute for New Materials	Saarbrücken
84	State Criminal Police Office Baden-Württemberg (LKA BW)	Stuttgart
85	University of Stuttgart	Stuttgart
86	Airbus Protect GmbH	Taufkirchen
87	Hensoldt Cyber GmbH	Taufkirchen
88	SkyFive AG	Taufkirchen
89	Airbus Defence and Space GmbH	Taufkirchen
90	Eberhard Karl University of Tübingen	Tübingen
91	eesy-innovation GmbH	Unterhaching
92	Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE	Wachtberg/Bonn
93	Hesse State Criminal Police Office (HLKA)	Wiesbaden
94	Hesse Police Headquarters for Technology (HPT)	Wiesbaden
95	Federal Criminal Police Office (BKA)	Wiesbaden/Berlin
96	University of Würzburg (JMU)	Würzburg

ILLUSTRATION: TAUSENDBLAUWERK.DE



Map legend

1	Location number of partners
●	Partner locations

Internationality

The RI CODE maintains a large international network. In 2023, employees came from 16 countries. We cooperated with 130 partners in 35 countries.

FIG.: ISTOCK / BLUE PLANET STUDIO

International Cooperation Partners

Country	Partner
Australia	University of Melbourne
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
	SBA Research
	TÜV TRUST IT GmbH
	University of Innsbruck
	University of Applied Sciences Campus Vienna
	University of Salzburg
	University of Vienna
	Vienna University of Technology
Belgium	EIT Digital
	KU Leuven
Canada	University of Toronto
	University of Waterloo
Croatia	Innovation Center Nikola Tesla (ICENT)
	University of Zagreb
Croatia	Utilis Ltd
Cyprus	Centre for Social Innovation Ltd. (CSI)
	Cyprus University of Technology (CUT)
	Eight Bells Ltd.
Czech Republic	Flowmon Networks AS
	IMA s.r.o.
	Masaryk University (MU)
Denmark	Aarhus University
Egypt	European Universities in Egypt
	German University in Cairo
Estonia	CybExer Technologies
	eu-LISA
	Foundation CR14
Finland	Jamk University of Applied Sciences
	Tampere University
	University of Oulu
France	ARIADNEXT
	Air and Space Force Academy Research Center (CREA)
	Cyber-Detect
	EURECOM
	Paris Cité University
	Thales SIX GTS France SAS

Country	Partner
France	University of Lorraine (UL)
Greece	Agroknow IKE
	Athena Research and Innovation Center (ARC)
	Centre for Research and Technology Hellas (CERTH)
	EXUS AI Labs
	Foodscale Hub
	Foundation for Research and Technology - Hellas (FORTH)
	Harokopio University of Athens
	IASIS NGO
	Logstail Mon. IKE
	Ministry of Digital Governance
	National and Kapodistrian University of Athens (NKUA)
	Space Hellas S.A.
	Ubitech
	University of Patras
Hungary	Eötvös Loránd University
Ireland	Trilateral Research Limited Ireland (TRI-IE)
Israel	Ben-Gurion University of the Negev
Italy	Abaco S.p.A.
	CRF
	CY4GATE S.p.A.
	Leonardo S.p.A.
	Polytechnic University of Turin
	Telecom Italia S.p.A.
	University of Bologna
	University of Insubria
	University of Milan
	University of Roma Tre
Japan	NTT Social Informatics Laboratories
Lithuania	Diversity Development Group
Luxembourg	University of Luxembourg
Malta	University of Malta (UM)
Netherlands	Airbus Defence and Space Netherlands B.V.
	Aircision BV
	Arthur's Legal B.V.
	Delft University of Technology
	Dutch Organization for Applied Scientific Research
	Eindhoven University of Technology (TU/e)
	SIDN - Stichting Internet Domeinregistratie Nederland
	SURFnet
	University of Groningen
	University of Twente
New Zealand	University of Auckland

Country	Partner
Norway	Norwegian University of Science and Technology (NTNU)
	Oslo Metropolitan University (Oslomet)
	Telenor ASA
	University of Oslo
Poland	Wroclaw University of Science and Technology (WUST)
Portugal	EFACEC Electric Mobility SA
Romania	Babeș-Bolyai University
	BitDefender SRL
Serbia	Foodscale Hub
Slovenia	Jožef Stefan Institute (JSI)
	University of Maribor
South Korea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Spain	Association Fòrum Dona Activa 2010
	Atos Spain S.A.
	Autonomous University of Madrid (UAM)
	CaixaBank, S.A.
	i2CAT
	Indra Sistemas S.A.
	NTT Data
	Telefónica I+D SA
	University of Murcia
Sweden	Ericsson AB
	RISE Research Institutes of Sweden AB
Switzerland	EPFL
	ETH Zurich
	RUAG
	University of Lausanne
	University of Zurich (UZH)
United Kingdom	Imperial College of Science, Technology and Medicine
	Lancaster University
	Trilateral Research Limited UK (TRI-IE)
	University of Glasgow
	University of Sheffield
	University of Surrey
USA	Auburn University, College of Engineering
	Brave Software
	Brown University
	Social Engineer Inc.
	University of Arizona, College of Engineering
	University of Maryland
	University of North Carolina at Charlotte
	University of Utah

FIG.: ADOBE STOCK / MH.DESING

Young Science

Offers and Opportunities

Study Award of the Research Institute CODE 2023

An Approach to Creating Adversarial Samples

Together with Giesecke+Devrient GmbH, the Research Institute CODE honors Mr. Hannes Jost Ludwig with the CODE Study Award 2023. In his Master‘s thesis, the cybersecurity student deals with ways of manipulating input data for Artificial Intelligence.

THE INCREASING INTEGRATION of artificial intelligence (AI) in everyday applications and its continuous further development are shaping the image of modern information technology (IT). On the one hand, this development offers a wide range of opportunities to society. On the other, it also brings up a number of new challenges, particularly in the area of IT security. These new security concerns must be addressed, particularly due to the growing dependence on AI.

In his Master's thesis "An Approach to Creating Adversarial Samples", Mr. Ludwig addresses these challenges by examining two key research topics in the security context: Adversarial Samples and Explainable AI. Adversarial samples are manipulated inputs that aim to disrupt neural networks and cause misclassifications. Adversarial samples therefore pose a potential security threat in numerous AI applications. Explainable AI aims to make AI models explainable, i.e., to make the decision-making processes of AI-based systems comprehensible and transparent.

The thesis focuses on how Explainable AI can contribute to the generation of adversarial samples. Theoretical approaches as well as practical applications are examined, including the integration of techniques from the field of image optimization. Parallels are drawn between this field and the generation of adversarial samples and provide new insights for more effective generation. In addition, the extent to which new attack methods on AI systems can be introduced through the generation of adversarial samples is investigated.

Mr. Ludwig's Master's thesis makes a decisive contribution to the current discussion on the security and transparency of AI systems. At the intersection between smart data and cyber defense, the thesis is characterized by a high degree of difficulty and critical reflection, as well as being highly topical. By developing new methods of generating manipulative inputs, the work promotes the demand for robustness and reliability of neural networks. At the same time, a deeper understanding of how AI technologies work is promoted by considering explainability. His work shows and illustrates that unsolved security problems still exist and that his approach is in principle very broadly applicable. Mr. Ludwig thus lays the foundation for further investigations on the use of explainable AI in the research area of adversarial samples.

The CODE Study Award was presented by University's Vice President Prof. Dr. Geralt Siebert in the presence of CODE Executive Director Prof. Dr. Wolfgang Hommel as well as the Technical Director of RI CODE Prof. Dr. Michaela Geierhos and Dr. Michael Tagscherer from Giesecke+Devrient during the grand master's ceremony on December 9, 2023, on the campus of the University of the Bundeswehr Munich. ■

CODE Study Award 2023 ceremony: Prof. Dr. Geralt Siebert, Prof. Dr. Wolfgang Hommel, award winner Hannes Ludwig, Prof. Dr. Michaela Geierhos, Dr. Michael Tagscherer (from left to right).

FIG.: ADOBE STOCK / TREECHA; UNIVERSITÄT DER BUNDESWEHR MÜNCHEN / 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

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 FH) in the STEM field as well as successful participation in a selection process conducted by the Assessmentcenter für Führungskräfte der 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
(in German)

FIG.: CLAUS SCHUNK

DOCTORATES 2023

Yasmeen Abdrabou

"Leveraging Eye Gaze to Enhance Security Mechanisms"

DESPITE THEIR security issues, such as weak and reused passwords, passwords remain a ubiquitous authentication approach. Notably, gaze patterns reveal several user traits. This thesis utilizes gaze behavior to enhance security mechanisms with a focus on knowledge-based passwords. We study password creation and its relation to cognitive load, then apply machine learning models to capture users' behavior, proposing a framework for using eye gaze in security systems and discussing ethical and privacy concerns.

Yasmeen Abdrabou received her doctorate in March 2023 under Prof. Dr. Florian Alt. She is currently employed at Lancaster University as a Senior Research Associate. ■

Michael Grabatin

"Architecture and Tools for Self-sovereign Identity Management on Distributed Ledgers"

THE THESIS describes a concept for self-sovereign identity management systems. It places the users at the center of all identity management operations, which increases transparency in the handling and interoperability of identity data. The identities created in this way can not only be used for browsing the Internet, but also for applications in the Internet of Things (IoT) and for electronic identities (eID). The thesis describes the required components and summarizes them into a comprehensive concept. Prototypical implementations are used to demonstrate the suitability of the concept. The thesis thus shows possible developments for secure and data protection-friendly identity management.

Michael Grabatin received his doctorate in December 2023 with Prof. Dr. Wolfgang Hommel as his primary advisor. He now works as a postdoc in the university's computer science department. ■

Joschka Kersting

"Identification of quantifiable Review Contents and Categories via Text Mining"

READING BETWEEN the lines has so far been reserved for humans, yet many texts on interpersonal topics are created online. The thesis addresses this research gap using machine learning methods. The goal is to identify and classify evaluative statements in order to relate them to other data. Organizations can thus analyze their services in a targeted manner. The results of the thesis lay a foundation for the automated quantification of implicit content, which was previously largely closed to machine processing.

Joschka Kersting received his Ph.D. in April 2023 under Prof. Dr. Michaela Geierhos. Currently, he is working in the Collaborative Research Centre (CRC) 901 "On-The-Fly Computing" at the Paderborn University. ■

Nils Mäurer

"Secure Communications in Next Generation Digital Aeronautical Datalinks"

TO MODERNIZE communications in civil aviation, new digital data links like the L-band Digital Aeronautical Communications System (LDACS) are introduced as of 2022. LDACS is a cellular, ground-based digital communications system for flight guidance and safety. This thesis proposes a cybersecurity architecture for LDACS. Novelties include two new authentication and key establishment protocols and a new method to secure control data of resource-constrained wireless communication systems. These security solutions enable future aeronautical applications, paving the way for a digitized and automated future of civil aviation.

Nils Mäurer received his doctorate in May 2023 under Prof. Dr. Gabi Dreo Rodosek. Currently, he is Technical Lead for IRIS2 at Airbus Defence and Space. ■

ALL FIG.: PRIVAT

Lukas Mecke

"User-centered Biometric Interfaces"

BIOMETRIC METHODS make use of unique patterns in user physiology or behavior for the purpose of authentication. However, users get little insight into what constitutes model decisions or control over this authentication mechanism. We propose a user-centered approach to both enhance existing interfaces with biometric systems and propose new ones with the aim to facilitate user literacy and agency over the recognition process and support the secure and informed use of biometrics.

Lukas Mecke received his doctorate in December 2023 under Prof. Dr. Florian Alt. He is currently employed at the Research Institute CODE as scientific staff member. ■

Tai Le Quy

"Fairness-aware Machine Learning in Educational Data Mining"

IN Educational Data Mining (EDM), machine learning-based decisions can be based on protected attributes. We perform a bias-aware analysis using Bayesian networks to understand bias in the datasets and evaluate group fairness measures in predictive models in student performance prediction problems. Next, we introduce the fair-capacitated clustering problem and the multi-fair capacitated students-topics grouping problem considering students' preferences, cardinalities and fairness. We show that bias-aware data analysis, fairness-aware models and measures are essential to ensure fairness in EDM.

Tai Le Quy received his doctorate in October 2023 under Prof. Dr. Eirini Ntoutsi and Prof. Dr. Gunnar Friege. Currently, he is a lecturer at the International University of Applied Sciences. ■

ALL FIG.: FI CODE / B. BELLGRAU

Capture the Flag 2023

“T 50 OO – Rise of the Machines”

On November 24 and 25, 2023, the Research Institute CODE hosted its ninth annual Capture the Flag event, which is organized together with Team localos and ITIS e.V. Over 100 people in 26 teams competed against each other in various challenges during the 18-hour event.

AT THE END OF NOVEMBER, after intense organisational preparation and an exciting qualification process in which almost 60 teams took part, the wait was over: A total of 26 teams arrived at the UniCasino on the campus of the University of the Bundeswehr Munich (UniBw M) on Friday evening to take part in the ninth edition of the “Capture the Flag” (CTF) event.

For many, the hacking competition, which has been held annually since 2015, has already established itself as a fixed date, as it combines skills training in the field of cyber security with lots of fun and action in an entertaining way. This year, the organizers from RI CODE, Team localos and ITIS e. V. had once again come up with some great ideas. A series of exciting tasks (known as “challenges”) had been worked out over the past weeks and months, which were to demand all the skill and dexterity of the more than 100 CTF participants. With the motto “T50OO - Rise of the Machines”, the event was themed around the “Terminator” film series. All challenges were thematically based on the plot of the action classic. At the same time, with the number 50 in the motto, the organizers managed to create a link to the 50th anniversary of UniBw M, which was celebrated in 2023.

At 6 p.m. on the dot, the Executive Director of RI CODE, Prof. Dr. Wolfgang Hommel, gave the official starting signal. The more than 40 varied challenges included tasks in both virtual and physical space. Time was the decisive factor here. Points were awarded depending on how quickly the teams were able to solve the tasks and puzzles. Teams that were the first to solve a challenge received extra points (“first blood”) and thus a valuable boost in the race to the top. As in the previous year, an exciting competition quickly developed between the best teams, which continued throughout the night and was not decided until the morning.

At the end of the 18-hour competition, the team “Pink Fluffy Unicorns” came out on top with 1,208 points, just ahead of the teams “SIGTERM;” (1,155 points) and “Pallas Athena CTF” (1,044 points). CODE’s Executive Director Prof. Dr. Wolfgang Hommel and CODE Managing Director Marcus Knüpfer congratulated the three top-placed teams on their great success and presented the happy winners with the prestigious Flag of Fame, on which all team members were allowed to proudly immortalize themselves with their signatures at the end.

A big thank you from the organizers goes last but not least to the numerous supporters, without whose generosity the event wouldn’t have been possible without one or two amenities. ■

What is a “Capture the Flag” (CTF) competition?

CTFS OFFER THE OPPORTUNITY to develop skills in the field of cyber security in a playful way and thus contribute to the practical training of experts.

RI CODE’s “Capture the Flag” is a hacking competition focusing on knowledge acquisition, team building and fun, which has been held once a year since 2015 on the campus of the University of the Bundeswehr Munich in Neubiberg. During the event, students can put their theoretical knowledge to the test by taking part in various practical challenges.

CODE Managing Director Marcus Knüpfer (left) and the CODE Executive Director, Prof. Dr. Wolfgang Hommel (right), presented the Flag of Fame to two representatives of the winning team “Pink Fluffy Unicorns” (center).

Among other tasks, the teams also had to pass a VR challenge at the CTF.

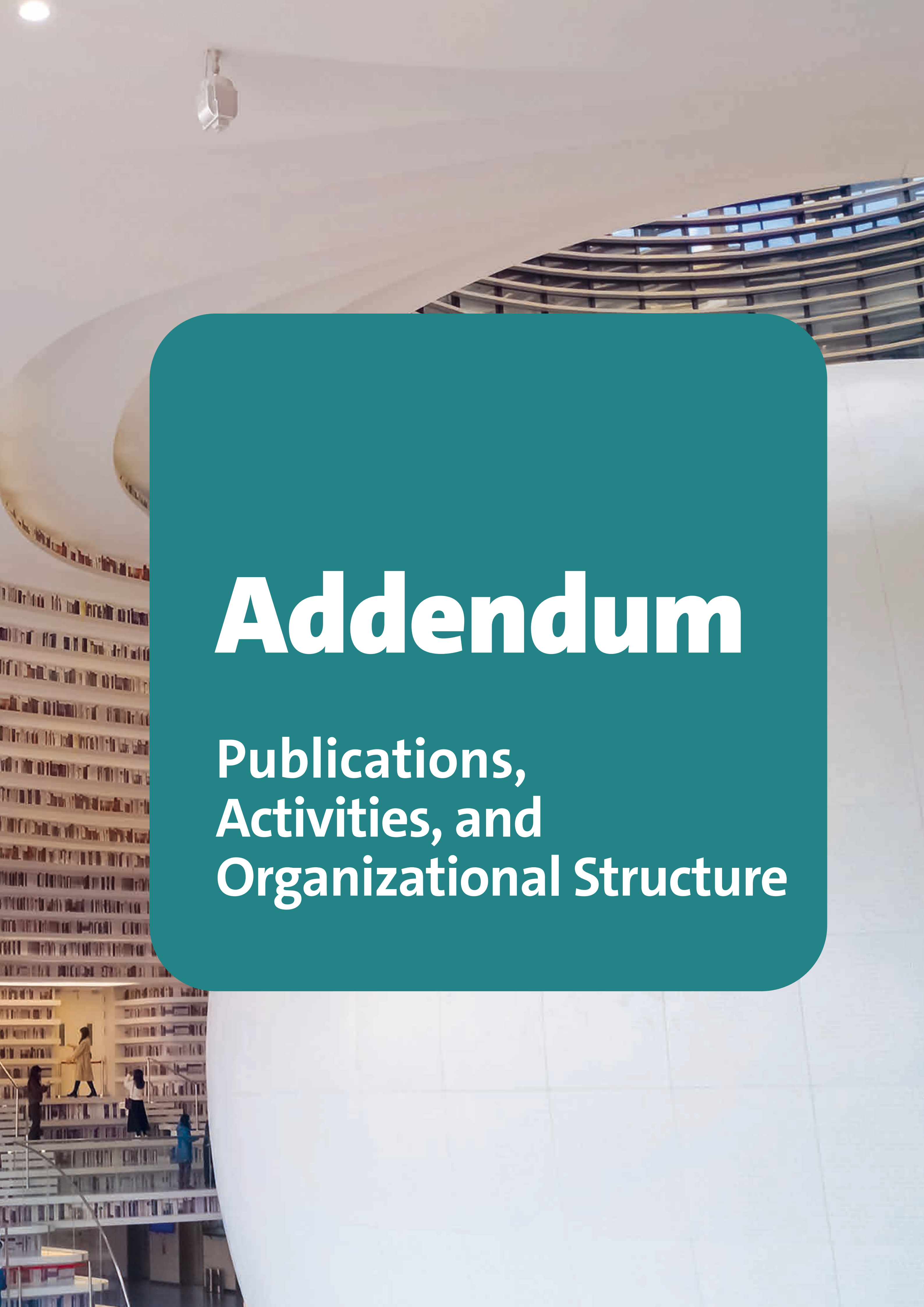
More information:

www.unibw.de/code/events/ctf

www.unibw.de/code/events/capture-the-flag-2023

@ ctf@unibw.de

FIG.: ADOBE STOCK / COWARD LION



Addendum

Publications, Activities, and Organizational Structure

Prof. Dr. Florian Alt

Usable Security and Privacy

PUBLICATIONS

ABDRABOU, Y., ASBECK, M., PFEUFFER, K., ABDELRAHMAN, Y., HASSIB, M., ALT, F.: Empowering Users: Leveraging Interface Cues to Enhance Password Security. In: Proceedings of the 19th IFIP TC 13 International Conference on Human-Computer Interaction (INTERACT '23), Springer, Berlin-Heidelberg, Germany, 2023.

ABDRABOU, Y., DIETZ, F., SHAMS, A., KNIERIM, P., ABDELRAHMAN, Y., PFEUFFER, K., HASSIB, M., ALT, F.: Revealing the Hidden Effects of Phishing Emails: An Analysis of Eye and Mouse Movements in Email Sorting Tasks, 2023.

ABDRABOU, Y., KARYPIDOU, E., ALT, F., HASSIB, M.: Investigating User Behaviour Towards Fake News on Social Media Using Eye Tracking and Mouse Movements. In: Proceedings of the Usable Security Mini Conference 2023 (USEC'23), Internet Society, San Diego, CA, USA, 2023. doi: https://dx.doi.org/10.14722/usec.2023.232041

ABDRABOU, Y., MECKE, L., RADIAH, R., PRANGE, S., NGUYEN, Q. D., VOIGT, V., ALT, F., PFEUFFER, K.: How Unique Do We Move? Understanding the Human Body and Context Factors for User Identification. In: Proceedings of Mensch und Computer 2023 (MuC '23), Association for Computing Machinery, New York, NY, USA, 2023, p. 127–137. doi:10.1145/3603555.3603574

ALT, F., HASSIB, M., DISTLER, V.: Human-centered Behavioral and Physiological Security. In: Proceedings of the 2023 Workshop on New Security Paradigms (NSPW '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3633500.3633504

DELGADO RODRIGUEZ, S., DAO PHUONG, A., BUMILLER, F., MECKE, L., DIETZ, F., ALT, F., HASSIB, M.: Padlock, the Universal Security Symbol? – Exploring Symbols and Metaphors for Privacy and Security. In: Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia (MUM '23), Association for Computing Machinery, New York, NY, USA, 2023.

DELGADO RODRIGUEZ, S., HEIN, O., PRIETO ROMERO, I., MECKE, L., DIETZ, F., PRANGE, S., ALT, F.: Shake-it-All: A Toolkit for Sensing Tangible Interactions on Everyday Objects. In: Workshop Beyond Prototyping Boards: Future paradigms for electronics toolkits (CHI '23 Workshops), 2023.

DELGADO RODRIGUEZ, S., RADIAH, R., MÄKELÄ, V., ALT, F.: Challenges in Virtual Reality Studies: Ethics and Internal and External Validity. In: Proceedings of the Augmented Humans International Conference 2023 (AHs '23), Association for Computing Machinery, New York, NY, USA, 2023, pp. 105–111. doi:10.1145/3582700.3582716

DISTLER, V., ABDRABOU, Y., DIETZ, F., ALT, F.: Triggering Empathy out of Malicious Intent: The Role of Empathy in Social Engineering Attacks. In: Proceedings of the 2nd Empathy-centric Design Workshop (EMPATHICH '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3588967.3588969

FLEISCHHAUER, Y., SURALE, H. B., ALT, F., PFEUFFER, K.: Gaze-based Mode-switching to Enhance Interaction with Menus on Tablets. In: Proceedings of the 2023 ACM Symposium on Eye Tracking Research & Applications (ETRA '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3588015.3588409

FROEHLICH, M., VEGA, J., PAHL, A., LOTZ, S., ALT, F., SCHMIDT, A., WELPE, I.: Prototyping with Blockchain: A Case Study for Teaching Blockchain Application Development at University. In: Learning in the age of digital and green transition (ICL '22), Springer International Publishing, Cham, 2023, pp. 1005–1017. doi:10.1007/978-3-031-26876-2_94

HEIN, O., RAUSCHNABEL, P., HASSIB, M., ALT, F.: Sick in the Car, Sick in VR?: Understanding how Real-World Susceptibility to Dizziness, Nausea and Eye Strain Influences VR Motion Sickness. In: Human-Computer Interaction – INTERACT 2023 (INTERACT '23), Springer Nature, Cham, Switzerland, 2023.

LIEBERS, J., GRUENEFELD, U., BUSCHEK, D., ALT, F., SCHNEEGASS, S.: Introduction to Authentication Using Behavioral Biometrics. In: Extended Abstracts of the 2023CHI Conference on Human Factors in Computing Systems (CHI EA '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3544549.3574190

MANSOUR, S., KNIERIM, P., O'HAGAN, J., ALT, F., MATHIS, F.: BANS: Evaluation of Bystander Awareness Notification Systems for Productivity in VR. In: Proceedings of the Usable Security Mini Conference 2023 (USEC'23), Internet Society, San Diego, CA, USA, 2023. doi:10.14722/usec.2023.234566

MECKE, L., PRIETO ROMERO, I., DELGADO RODRIGUEZ, S., ALT, F.: Exploring the Use of Electromagnets to Influence Key Targeting on Physical Keyboards. In: Extended abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3544549.3585703

NAMNAKANI, O., SINRATTANAVONG, P., ABDRABOU, Y., BULLING, A., ALT, F., KHAMIS, M.: Gazecast: Using Mobile Devices to Allow Gaze-based Interaction on Public Displays. In: Proceedings of the 2023 ACM Symposium on Eye Tracking Research & Applications (ETRA '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3588015.3589663

PFEUFFER, K., OBERNOLTE, J., DIETZ, F., MÄKELÄ, V., SIDENMARK, L., MANAKHOV, P., PAKANEN, M., ALT, F.: PalmGazer: Unimanual Eye-Hand Menus in Augmented Reality. In: Proceedings of the 2023 ACM Symposium on Spatial User Interaction (SUI '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3607822.3614523

PRANGE, S., ALT, F.: Increasing Users' Privacy Awareness in the Internet of Things: Design Space and Sample Scenarios. In: Human Factors in Privacy Research, N. Gerber, A. Stöver, and K. Marky, Eds., Cham: Springer International Publishing, 2023, pp. 321–336. doi:10.1007/978-3-031-28643-8_16

RADIAH, R., PRODAN, P., MÄKELÄ, V., KNIERIM, P., ALT, F.: How Are Your Participants Feeling Today? Accounting For and Assessing Emotions in Virtual Reality. In: Proceedings of Mensch und Computer 2023 (MuC '23), Association for Computing Machinery, New York, NY, USA, 2023, pp. 37–48. doi:10.1145/3603555.3603577

RADIAH, R., ROTH, D., ALT, F., ABDELRAHMAN, Y.: The Influence of Avatar Personalization on Emotions in VR. Multimodal technologies and interaction, vol. 7, iss. 4, 2023. doi:10.3390/mti7040038

SAAD, A., IZADI, K., KHAN, A. A., KNIERIM, P., SCHNEEGASS, S., ALT, F., ABDELRAHMAN, Y.: HotFoot: Foot-based User Identification Using Thermal Imaging. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), Association for Computing Machinery, New York, NY, USA, 2023. doi:10.1145/3544548.3580924

TEUSCHEL, M., PÖHN, D., GRABATIN, M., DIETZ, F., HOMMEL, W., ALT, F.: "Don't Annoy Me With Privacy Decisions!" – Designing Privacy-Preserving User Interfaces for SSI Wallets on Smartphones. IEEE Access, vol. 11, pp. 131814-131835, 2023. doi:10.1109/ACCESS.2023.3334908

VOIGT, V., WIETHE, R., SASSMANN, C., WILL, M., DELGADO RODRIGUEZ, S., ALT, F.: Safe Call: A Tangible Smartphone Interface that Supports Safe and Easy Phone Calls and Contacts Management for Older People. In: Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia (MUM '23), Association for Computing Machinery, New York, NY, USA, 2023.

RESEARCH PROJECTS

Voice of Wisdom

The Voice of Wisdom project explores approaches to prevent human-centric cyberattacks. By analyzing human behavior and physiological states, signs that people are at risk are identified. In addition, novel human-centric security mechanisms are being developed and the long-term effects of these are being studied.

Funded by: dtec.bw

Duration: 01/2021 – 12/2024

PrEvoke – Supporting Users in Informed Privacy Permission Revocation

PrEvoke addresses the consequences of revoking privacy decisions (e.g., when users revoke apps' access to personal data). The consequences expected by users with regard to the revocation of privacy permissions are examined and compared with reality. Appropriate concepts are also created to counter misunderstandings and concerns.

Funded by: Google München

Duration: 12/2021 – 12/2023

Scalable Biometrics

The Scalable Biometrics project explores how pervasive computing environments can leverage behavioral biometrics for identifying and authenticating users. The main question is how behavioral biometrics approaches scale to different pervasive computing environments, containing multiple users with changing behavior, different physicalities, and changing sensing and interaction capabilities.

Funded by: DFG

Duration: 04/2020 – 03/2023

ubihave

Ubiquitous computers serve as both everyday companions and environmental sensors. Such devices generate user-specific data, enabling the creation of behavioral models and applications. This project develops models that describe, analyze and predict user behavior. Promising application areas are: usable security, touch interaction, text input, and context-sensitive, adaptive systems.

Funded by: DFG

Duration: 01/2019 – 02/2023

TEACHING

10123	**Human Factors in Computing Systems**
39181	**Usable Security**
39182	**Practical Course Design of Usable and Secure System**
39183	**Secure Human-Computer Interfaces**
55011	**Research Methods in Usable Security**

FAIRS, CONFERENCES, SEMINARS

- USEC Summer School on Usable Security and Privacy
- Dagstuhl Seminar on Social Engineering
- Winter School on Human-Centered Security
- CHI 2023 Course on Authentication Using Behavioral Biometrics
- Tangible Interactions Workshop (Mensch und Computer 2023)
- VHS Course: Smart Home Security (50 years University of the Bundeswehr)
- Cyber Awareness Training (NATO JSEC)
- International Doctoral Seminar with TU Wien in Ramenai

PRIZES AND AWARDS

- ACM Symposium on Spatial User Interaction (SUI'23) - Honorable Mention: Pfeuffer, K., Obernolte, J., Dietz, F., Mäkelä, V., Sidenmark, L., Manakhov, P., Pakanen, M., Alt, F.: PalmGazer: Unimanual Eye-Hand Menus in Augmented Reality.
- 2023 Communication by Gaze Interaction (COGAIN) Symposium - Best Paper Award: Namnakani, O., Sinrattanavong, P., Abdrabou, Y., Bulling, A., Alt, F., Khamis, M.: GazeCast: Using Mobile Devices to Allow Gaze-based Interaction on Public Displays.

ADDITIONAL FUNCTIONS

- PC Chair / Editor for ACM Interactive Surfaces and Spaces 2023/2024
- TPC Chair for Mensch und Computer 2023
- Program Committee Member for SOUPS 2023
- Guest Editor for IEEE Pervasive Computing Special Issue on the Pervasive Multiverse
- Department Editor for IEEE Pervasive Computing - Security & Privacy
- Editorial Board for IEEE Pervasive Computing
- Steering Committee Chair for Mobile and Ubiquitous Multimedia (MUM) Conference Series
- Keynote Speaker for Augmented Humans 2023

Prof. Dr.
Harald Baier

Digital Forensics

PUBLICATIONS

GÖBEL, T., BAIER, H., BREITINGER, F.: Data for Digital Forensics: Why a Discussion on "How Realistic is Synthetic Data" is Dispensable. Digital Threats 4, 3, Article 38 (September 2023), 18 pages. https://doi.org/10.1145/3609863

GONCALVES, P., BAIER, H.: Applying Activity-based Models to Integrate Labeled Preset Key Events in Intra-Day Human Mobility Scenarios. In: Proceedings of the 9th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS) 2023, Prague, Czech Republic, April 26–28, 2023, pp. 281–288.

KLIER, S., BAIER, H.: Scalable Image Clustering to Screen for Self-produced CSAM. AICSEC 2023 – EAI International Conference on Artificial Intelligence for CyberSecurity.

KLIER, S., BAIER, H.: To Possess or Not to Possess - WhatsApp on Android Revisited with a Focus on Stickers. NordSec 2023 – 28th Nordic Conference on Secure IT Systems.

KLIER, S., VARENKAMP, J., BAIER, H.: Back and Forth – On Automatic Exposure of Origin and Dissemination of Files on Windows. In: Digital Threats: Research and Practice 4.3 (2023): 1–17.

MUNDT, M., BAIER, H.: Abbildung und Simulation cyber-physischer Bedrohungen für kritische Infrastrukturen. In: Proceedings of the 30. DFN-Konferenz "Sicherheit in vernetzten Systemen", Hamburg, February 2023.

MUNDT, M., BAIER, H.: Enabling Protection Against Data Exfiltration by Implementing ISO 27001:2022 update. In: International Conference on Security & Applications (SECURA 2023), International Journal on Cybernetics & Informatics (IJCI), virtual, August 2023.

MUNDT, M., BAIER, H.: Enhancing Incident Management by an Improved Understanding of Data Exfiltration: Definition, Evaluation, Review. International Conference on Digital Forensics and Cyber Crime. In: Proceedings of the EAI ICDF2C 2023 – 14th EAI International Conference on Digital Forensics & Cyber Crime, New York City (USA), November 30–31, 2023.

MUNDT, M., BAIER, H.: Short contribution to Springer Encyclopedia about Data Exfiltration. Encyclopedia of Cryptography, Security and Privacy. April 2023.

TWENNING, L., BAIER, H., GÖBEL, T.: These ARE the Pictures You Are Looking for – On the Use of Perceptual Hashing in Targeted Content Scanning. In: Proceedings of the 19th Annual IFIP WG 11.9 International Conference on Digital Forensics, hybrid (Arlington USA), January 2023.

UHLIG, F., STRUPPEK, L., HINTERSDORF, D., GÖBEL, T., BAIER, H., KERSTING, K.: Combining AI and AM – Improving Approximate Matching Through Transformer Networks. In: Proceedings of the 23rd Annual DFRWS USA Conference, hybrid (Baltimore USA), July 2023.

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

- Local organization and conference chair of the IT forensics conference IMF 2023 in May 2023 in the UniCasino of the UniBw M, URL: https://imf-conference.org/imf2023/
- Preparation and moderation of the CAST workshop Forensics / Cybercrime on December 14, 2023, URL: https://cast-forum.de/workshops/infos/328
- Workshop (in cooperation with ZITiS) on drone forensics at the CODE Annual Conference and IMF 2023
- Presentation "Enhancing Incident Management by an Improved Understanding of Data Exfiltration: Definition, Evaluation, Review". 14th International Conference on Digital Forensics and Cybercrime (ICDF2C 2023), December 1,, 2023, New York, USA
- Presentation "Forensic Approach to Drones from the Manufacturers Parrot Anafi and Yuneec Typhoon". "Veitshöchheimer Runde", October 18,, 2023, Veitshöchheim, Germany
- Presentation "Forensic Analysis of a Parrot Anafi Drone". Drone workshop "Selected topics of drone forensics" at the CODE Annual Conference 2023, July 12, 2023, Neubiberg, Germany
- Presentation "Digital Forensics Between Yesterday and Tomorrow". Plenary lecture at the CODE Annual Conference 2023, July 11, 2023, Neubiberg, Germany
- Presentation "Forensics of Intelligent Systems". Keynote at the symposium "SIC! Security and Innovation in Cyberspace" of the Agentur für Innovation in der Cybersicherheit (Cyberagentur), June 20, 2023, Halle (Saale), Germany
- Presentation "Forensic Analysis of a Parrot Anafi UAV". Drone workshop "Data acquisition and analysis of UAVs (drones)" at the IMF 2023, May 24, 2023, Neubiberg, Germany
- Presentation "Using Perceptual Hashing in Targeted Content Scanning". 19th Annual IFIP Working Group 11.9 International Conference on Digital Forensics, January 31, 2023, Arlington, USA (online)

ADDITIONAL FUNCTIONS

- Reviewer for "Journal of Digital Investigation" and "Computers & Security"
- Membership in program committees: Digital Forensics Research Workshop (DFRWS) EU 2023, Digital Forensics Research Workshop (DFRWS) APAC 2023, IT Security Incident Management & IT Forensics (IMF) 2023, IFIP Working Group 11.9 International Conference on Digital Forensics 2023, CAST-GI Doctoral Award 2023
- Support of the program director in establishing the study program "IT Security" at the Vietnamese-German University in Ho-Chi-Minh City, Vietnam

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

PUBLICATIONS

BERLAKOVICH, F., BRUNTHALER, S.: R2C: AOCR-Resilient Diversity with Reactive and Reflective Camouflage. In: Proceedings of the Eighteenth European Conference on Computer Systems, EuroSys 2023, Rome, Italy, May 8-12, 2023. ACM 2023, pp. 488–504.

BERLAKOVICH, F., BRUNTHALER, S.: R2C: AOCR-Resilient Diversity with Reactive and Reflective Camouflage. In: Noll, Thomas; Fesefeldt, Ira (Ed.). 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung. Aachener Informatik-Berichte (AIB), AIB-2023-03.

BERNAD, M., BRUNTHALER, S.: HOBBIT – Hash-based Object Integrity. In: Noll, Thomas; Fesefeldt, Ira (Ed.). 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung. Aachener Informatik-Berichte (AIB), AIB-2023-03.

MECHELINCK, R., DORFMEISTER, D., FISCHER, B., VOLCKAERT, S., BRUNTHALER, S.: DEPS: Leveraging Hardware Faults for Binding Software to Hardware. In: Noll, Thomas; Fesefeldt, Ira (Ed.). 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung. Aachener Informatik-Berichte (AIB), AIB-2023-03.

MARKVICA, D., BRUNTHALER, S.: µWASM: Interpreting WebAssembly. In: Aachener Informatik-Berichte (AIB), AIB-2023-03, In: Noll, Thomas; Fesefeldt, Ira (Ed.). 22. Kolloquium Programmiersprachen und Grundlagen der Programmierung. Aachener Informatik-Berichte (AIB), AIB-2023-03.

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 – 2024

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 – 2024

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

- Network and Distributed Systems Symposium 2023, San Diego, CA, USA.
- IFIP Working Group 2.3 Workshop in York Harbor, MN, USA.
- European Conference on Computer Systems (EuroSys) 2023, in Rome, IT.
- European Symposium on Security & Privacy 2023, in Delft, NL.
- Kolloquium in Programmiersprachen und Systeme (KPS) 2023, in Vaals, NL.
- ACM Computer and Communications Symposium (CCS), 2023, in Copenhagen, Denmark.
- Organizer of the IFIP Working Group 2.4 Workshop #68.

ADDITIONAL FUNCTIONS

- Area Chair, Journal of Systems Research (JSys).
- Member IFIP Working Group 2.4, Software Implementation Technology.

Program Committees

- Network and Distributed Systems Symposium 2023, San Diego, CA, USA.
- European Symposium on Security & Privacy 2023, in Delft, NL.
- ACM Computer and Communications Symposium (CCS), 2023, in Copenhagen, Denmark.

Prof. Dr. Michaela Geierhos

Data Science

PUBLICATIONS

BÄUMER, F. S., BRANDT-POOK, H., MAORO, F., SCHULTENKÄMPER, S, STECKER, B. (2023). Von der Theorie zur Praxis: Erfahrungen bei der akademischen Begleitung von KI-Projekten in KMUs. In: Klein, M.; Krupka, D.; Winter, C.; Wohlgemuth, V. (Ed.). Designing Futures: Zukünfte gestalten. Informatik 2023. Lecture Notes in Informatics (LNI) – Proceedings. Köllen Druck+Verlag Bonn. 2023. pp. 1817–1828.

BÄUMER, F. S., CHEN, W.-F., GEIERHOS, M., KERSTING, J., WACHSMUTH, H. (2023). Subproject B1: Dialogue-based Requirement Compensation and Style-adjusted Data-to-Text Generation. In: Haake, C.-J.; Meyer auf der Heide, F.; Platzner, M.; Wachsmuth, H.; Wehrheim, H. (Ed.). On-the-Fly Computing – Individualized IT-services in Dynamic Markets. Verlagsreihenschriften des Heinz Nixdorf Instituts. pp. 65–84.

GEIERHOS, M. (2023). German Angst und Datensicherheit: Erwägungen über den passenden Umgang mit Patientendaten in Deutschland. In: Ferber, M.; Seidenath, B. (Ed.). Gesundheitsdaten nutzen! Für eine patientenwohlorientierte Versorgung von morgen. Aktuelle Analysen 94. Hanns-Seidel-Stiftung e.V. München. pp. 88–97.

HOMMEL, W., GEIERHOS, M., KNÜPFER, M., BELLGRAU, B., SCHREIBER, U., ZAHN, J. (2023). CODE-Jahrestagung 2023: Zehn Jahre Forschung und Vernetzung im Bereich Cybersicherheit. Zeitschrift für Außen- und Sicherheitspolitik.

KERSTING, J. (2023). Identifizierung quantifizierbarer Bewertungsinhalte und -kategorien mittels Text Mining. Monographie. Universität der Bundeswehr München. 2023. p. 208.

KERSTING, J., GEIERHOS, M. (2023). Towards Comparable Ratings: Quantifying Evaluative Phrases in Physicians Reviews. In: Cuzzocrea, Al; Gusikhin, O.; Hammoudi, S.; Quix, C. (Ed.). Data Management Technologies and Applications: 10th International Conference, DATA 2021, Virtual Event, July 6—8, 2021, and 11th International Conference, DATA 2022, Lisbon, Portugal, July 11—13, 2022, Revised Selected Papers. Communications in Computer and Information Science 1860. Springer 2023. Cham, Schweiz. pp. 45–65.

KERSTING, J., MAORO, F., GEIERHOS, M. (2023). Towards Comparable Ratings: Exploring Bias in German Physician Reviews. Data & Knowledge Engineering 148. pp. 102–235.

MEISSNER, A., FRÖHLICH, A., GEIERHOS, M. (2023). Keep it Simple: Evaluating Local Search-based Latent Space Editing. SN Computer Science 4, 820.

MERTEN, M.-L., WEVER, M., GEIERHOS, M., TOPHINKE, D., HÜLLERMEIER, E. (2023). Annotation Uncertainty in the Context of Grammatical Change. International Journal of Corpus Linguistics 28(3). pp. 430–459.

SCHULTENKÄMPER, S., BÄUMER, F. S., GEIERHOS, M., LEE, Y. S. (2023). From Unstructured Data to Digital Twins. From Tweets to Structured Knowledge. In: Jimenez, J. M. (Ed.). Proceedings of the Thirteenth International Conference on Social Media Technologies, Communication, and Informatics (SOTICS 2023). pp. 6–11.

SEEMANN, N., LEE, Y. S., HÖLLIG, J., GEIERHOS, M. (2023). Generalizability of Abusive Langue Detection Models on Homogeneous German Datasets. Datenbank-Spektrum 23(1). pp. 15–25.

SEEMANN, N., LEE, Y. S., HÖLLIG, J., GEIERHOS, M. (2023). The Problem of Varying Annotations to Identify Abusive Language in Social Media Content. Natural Language Engineering 29 (6). pp. 1561–1585.

ULLRICH, S., SOARES DE SOUZA, A., KÖHLER, J., GEIERHOS, M. (2023). BloomQDE: Leveraging Bloom's Taxonomy for Question Difficulty Estimation. In: Abbas, M. (Ed.). Analysis and Application of Natural Language and Speech Processing. Signals and Communication Technology. Springer 2023. Cham, Schweiz. pp. 145–155.

RESEARCH PROJECTS

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 – 12/2024

KIMONO – Campaign Identification, Monitoring and Classification Using Social Media Mining Methods for integration in an AI-based Early Warning System

The aim of the KIMONO project is the detection and modeling of short- and long-term disinformation and influence campaigns in social media such as X (formerly Twitter) and Facebook. In particular, the focus is on campaigns that are driven by stately actors.

Funded by: BMVg/BAAINBw
Duration: 09/2021 – 12/2024

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: BMBF

Duration: 02/2023 – 01/2026

MuQuaNet – Greater Munich Quantum Internet "Authority-Dependent Risk Identification and Analysis in online Networks"

The aim is to automatically monitor selected apps and analyze the data they collect, correlate it with social media profiles, and form networks of people in order to identify potential targets and classify their risk potential on the basis of given data.

Funded by: dtec.bw

Duration: 10/2020 – 12/2024

SFB 901 "On-the-fly Computing" "Parameterized Service Specification"

In the spirit of agile, participatory software development, end users are more involved in the interactive composition process of software services to be created on the fly. To this end, it must be made transparent to the user which requirements were taken into account during creation and which had to be omitted.

Funded by: German Research Foundation (DFG)

Duration: 07/2019 – 06/2023

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: BMBF

Duration: 01/2022 – 12/2024

TEACHING

1144 **Knowledge Discovery in Big Data**

3850 **Natural Language Processing**

3851 **Information Retrieval**

3852 **Data Science Applications**

FAIRS, CONFERENCES, SEMINARS

- Cyber Awareness Training (NATO JSEC, Ulm)
- Business Informatics Transfer Forum (HSBI, Bielefeld)
- KI@BW (HSU, Hamburg)

PRIZES AND AWARDS

- ICIST Best Paper Award
  Sergej Schultenkämper and Frederik S. Bäumer present a method that can be used to identify potential data protection risks in German patient forums.

ADDITIONAL FUNCTIONS

- Faculty council member
- Member of the Board of the Cyber Security Master's Program (since 12/2023)
- Member of the advisory board "German Biography" of the Historical Commission at the Bavarian Academy of Sciences and Humanities
- Expert for the European Commission
- Expert for VDI/VDE Innovation + Technik
- Reviewer for journals, e.g. Health Policy

Program Committee

- ACL 2023 – Annual Meeting of the Association for Computational Linguistics
- EMNLP 2023 – Conference on Empirical Methods in Natural Language Processing
- PATTERNS 2023 – International Conference on Pervasive Patterns and Applications
- SEMANTICS 2023 – International Conference on Semantic Systems

Prof. Dr. Marta Gomez-Barrero

BioML: Biometrics and Machine Learning Lab

PUBLICATIONS

BUSCH, C., DERAVI, F., FRINGS, D., KINDT, E., LESSMANN, R., NOUAK, A., SALOMON, J., ACHCAR, M., ALONSO-FERNANDEZ, F., BACHENHEIMER, D., BETHELL, D., BIGUN, J., BRAWLEY,M., BROCKMANN, G., CABELLO, E., CAMPISI, P., CEPILOVS, A., CLEE, M., COHEN, M., CROLL, C., CZYZEWSKI, A., DORIZZI, B., DRAHANSKY, M., DROZDOWSKI, P., FANKHAUSER, C., FIERREZ, J., GOMEZ-BARRERO, M., HASSE, G., GUEST, R., KOMLEVA, E., MARCEL, S., MARCIALIS, G. L., MERCIER, L., MORDINI, E., MOUILLE, S., NAVRATILOVA, P., ORTEGA-GARCIA, J., PETROVSKA, D., POH, N., RACZ, I., RAGHAVENDRA, R., RATHGEB, C., REMILLET, C., SEIDEL, U., SPREEUWERS, L., STRAND, B., TOIVONEN, S., UHL, A.: Facilitating Free Travel in the Schengen Area. IET Biometrics, 2023.

GONZALEZ-SOLER, L. J., GOMEZ-BARRERO, M., BUSCH, C.: Towards Generalisable Facial Presentation Attack Detection Using Facial Region Ensembles. IEEE Access, 2023.

GONZALEZ-SOLER, L. J., GOMEZ-BARRERO, M., PATINO, J., TODISCO, M., EVANS, N., BUSCH, C.: Fisher Vectors for Biometric Presentation Attack Detection. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment, pp. 489–519, 2023.

MORALES, A., FIERREZ, J., GALBALLY, J., GOMEZ-BARRERO, M.: Introduction to Iris Presentation Attack Detection in Iris Biometrics and Recent Advances. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment, pp. 103–121, 2023.

RAJA, K., RAGHAVENDRA, R., VENKATESH, S., GOMEZ-BARRERO, M., RATHGEB, C., BUSCH, C.: Vision Transformers Against CNNs for Fingerprint Presentation Attack Detection: Generalizability and Explainability. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment, pp. 17-56, 2023.

FAIRS, CONFERENCES, SEMINARS

- IEEE Int. Conference of the Biometrics Special Interest Group (BIOSIG) (General Chair)
- IEEE Int. Joint Conference on Biometrics (IJCB) (Publication Chair)
- IEEE Int. Workshop on Biometrics and Forensics (WIFS) (General 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 Standardisation (DIN) in ISO/IEC SC37 JTC1 SC37 on biometrics
- Co-Affiliation Norwegian University of Science and Technology (NTNU)

Prof. Dr. Udo Helmbrecht

Quantum Communication

PUBLICATIONS

FARINA, F., RÖHRICH, S., RÖDIGER, J., KÖRFGEN, H.: QKD Key Management for Military Applications: A Study in the MuQuaNet Testbed. IST-SET-198-RSY on Quantum Technology for Defence and Security, October 3–4, 2023 – Amsterdam, Netherlands.

SCHATZ, D., ALTHEIDE, F., KÖRFGEN, H., ROSSBERG, M., SCHÄFER, G.: Virtual Private Networks in the Quantum Era: A Security in Depth Approach. SECRYPT 2023 – The 20th International Conference on Security and Cryptography, July 10–12, 2023 – Rome, Italy.

TEACHING

3695 **Quantum Communication**

FAIRS, CONFERENCES, SEMINARS

- DPG Spring Meetings 2023
- IST-SET-198-RSY on Quantum Technology for Defence and Security in Amsterdam
- QBN Quantum Industry Summit in Stuttgart
- BWI Quantensymposium in Berlin
- ZITiS TechZoom in Munich
- QR.X workshop on the implementation of fiber channels for quantum communications

Prof. Dr. Wolfgang Hommel

Software and Data Security

PUBLICATIONS

DIETERICH, A., SCHOPP, M., STIEMERT, L., STEININGER, C., PÖHN, D.: Evaluation of Persistence Methods Used by Malware on Microsoft Windows Systems. Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP). Setúbal: SciTePress. 2023. pp. 552–559.

DIMARATOS, A., PÖHN, D.: Evaluation Scheme to Analyze Keystroke Dynamics Methods. In: Mori, Paolo; Lenzini, Gabriele; Furnell, Steven (Ed.). Proceedings of the 9th International Conference on Information Systems Security and Privacy – ICISSP. Setúbal: SciTePress. 2023. pp.357–365.

EIPPER, A., PÖHN, D.: How to Design a Blue Team Scenario for Beginners on the Example of Brute-Force Attacks on Authentications. In: Mori, Paolo; Lenzini, Gabriele; Furnell, Steven (Ed.). Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP). Setúbal: SciTePress. 2023. pp. 477–484.

FRANK, A., HOMMEL, W., HOPFNER, B.: An Intermediary Protocol Representation to Aid in Avionics Network Development. Proceedings of IEEE/IFIP Network Operations and Management Symposium 2023. Piscataway, NJ. IEEE. 2023. pp. 1–5.

GAMISCH, L., PÖHN, D.: A Study of Different Awareness Campaigns in a Company. ARES ‘23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA: Association for Computing Machinery. 2023. pp. 68.

HAFNER, L., WUTZ, F., PÖHN, D., HOMMEL, W.: TASEP: A Collaborative Social Engineering Tabletop Role-playing Game to Prevent Successful Social Engineering Attacks. ARES ‘23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA: Association for Computing Machinery. 2023. pp. 67.

MAKOWSKI, J.-P., PÖHN, D.: Evaluation of Real-World Risk-based Authentication at Online Services Revisited. ARES ‘23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA. Association for Computing Machinery. 2023. pp. 73.

PÖHN, D., GRABATIN, M., HOMMEL, W.: Modeling the Threats to Self-sovereign Identities. in: Roßnagel, Heiko; Schunck, Christian H.; Günther, Jochen (Ed.). Open Identity Summit 2023. Bonn. Gesellschaft für Informatik e.V. 2023. pp. 85–96.

PÖHN, D., GRUSCHKA, N., ZIEGLER, L., BÜTTNER, A.: A Framework for Analyzing Authentication Risks in Account Networks. Computers & Security. Vol. 135. 2023. pp. 103515.

PÖHN, D., HOMMEL, W.: New Directions and Challenges within Identity and Access Management. IEEE Communications Standards Magazine. Piscataway, NJ. IEEE. Vol. 7. 2023. No. 2. pp. 84–90.

PÖHN, D., HOMMEL, W.: Towards an Improved Taxonomy of Attacks Related to Digital Identities and Identity Management Systems. Security and Communication Networks. 2023. Special Conference Issue: Interdisciplinary and Sustainable Cybersecurity.

PÖHN, D., MÖRSDORF, N., HOMMEL, W.: Needle in the Haystack: Analyzing the Right of Access According to GDPR Article 15 Five Years after the Implementation. ARES ‘23: Proceedings of the 18th International Conference on Availability, Reliability and Security. New York, NY, USA: Association for Computing Machinery. 2023. pp. 91.

PÖHN, D., SEEBER, S., HOMMEL, W.: Combining SABSA and Vis4Sec to the Process Framework IdMSecMan to Continuously Improve Identity Management Security in Heterogeneous ICT Infrastructures. Applied Sciences. Vol. 13. 2023. No. 4. pp. 2349.

TEUSCHEL, M., PÖHN, D., GRABATIN, M., DIETZ, F., HOMMEL, W., ALT, F.: ‘Don’t Annoy Me With Privacy Decisions!’ — Designing Privacy-preserving User Interfaces for SSI Wallets on Smartphones. IEEE Access. Piscataway, NJ. IEEE. Vol. 11. 2023. pp. 131814–131835.

WALKOW, M., PÖHN, D.: Systematically Searching for Identity-Related Information in the Internet with OSINT Tools. In: Mori, Paolo; Lenzini, Gabriele; Furnell, Steven (Ed.). Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP). Setúbal: SciTePress. 2023. pp. 402–409.

RESEARCH PROJECTS

6G-life

The 6G-life project uses a holistic approach to research innovative concepts in the field of scalable communication, new methods, flexible software concepts and adaptive hardware that support the basic idea of human-machine collaboration. In all research fields, the requirements for latency, resilience, security and sustainability are always addressed in parallel as multidisciplinary topics.

Funded by: BMBF (subcontracted by TU Munich)
Duration: 12/2022 – 08/2025

DEFINE – DC-Netze für eine sichere Energieversorgung

Modern power grids are fed from renewable power sources such as solar or wind energy and serve increasingly demanding needs such as electromobility. Direct current distribution grids promise an advantage over conventional AC grids regarding efficiency and control. RI CODE is researching hardened IT and suitable monitoring just as control solutions for these future energy supply grids.

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw (funded by the European Union – Next Generation EU)
Duration: 01/2021 – 12/2024

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 – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw (funded by the European Union – Next Generation EU)
Duration: 01/2021 – 12/2024

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

The R&T study Technical Adaptation of Cyber Ranges for Military Use 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: Bundeswehr Technical Center for Information Technology and Electronics in the Bundeswehr (WTD81)
Duration: 10/2023 – 06/2025

TEACHING

1006	**Introduction to Computer Science 1**
1007	**Introduction to Computer Science 2**
3459	**Selected Chapters of IT Security**
5501	**Seminar Application and Software Security**
5501	**Seminar Information Security Management**
5507	**Secure Networked Applications**
5508	**Information Security Management**

ADDITIONAL FUNCTIONS

- Board of examiners for Master of Intelligence & Security Studies
- Member of the Operating Committee of the German Research and Education Network
- Expert in the research funding program “Sparkling Science 2.0”

Program Committee

- IEEE/IFIP International Symposium on Integrated Network Management
- IEEE/IFIP Network Operations and Management Symposium
- IEEE International Conference on Communications
- DFN Conference Security in Networked Systems
- Workshop on Avionics Systems and Software Engineering
- International Workshop on Frontiers in Availability, Reliability and Security
- International Journal of Critical Infrastructure Protection
- International Journal of Electronic Government
- International Journal of Innovation and Technology Management

Prof. Dr.-Ing.
Mark Manulis

Privacy and Applied Cryptography Lab

PUBLICATIONS

GARDHAM, D., MANULIS, M.: Generalised Asynchronous Remote Key Generation for Pairing-based Cryptosystems. Applied Cryptography and Network Security – 21st International Conference, ACNS 2023, Kyoto, Japan, June 19-22, 2023, Proceedings, Part I, Springer, 2023: pp. 394–421.

FRYMANN, N., GARDHAM, D., MANULIS, M.: Asynchronous Remote Key Generation for Post-Quantum Cryptosystems, 8th IEEE European Symposium on Security and Privacy, EuroS&P 2023, Delft, Netherlands, July 3-7, 2023: pp. 928–941.

RESEARCH PROJECTS

EU H2020 Project SECANT: Security and Privacy Protection in Internet of Things Devices

The project is developing an innovative cybersecurity risk assessment platform to address cascading cyber threats and increase privacy and data protection across the connected ICT ecosystem. PACY Lab is working on cryptographic protocols based on blockchain technology to enable privacy-preserving search over encrypted sensitive data.

Funded by: EU H2020
Duration: 09/2021 – 08/2024
Participation via University of Surrey, UK

TEACHING

55481	**Modern Cryptography**
55482	**Seminar Research Trends in Cryptography**
55631	**Private Data Processing**
55632	**Private Authentication and Messaging**
55633	**Seminar Privacy Enhancing Cryptography in Practice**

ADDITIONAL FUNCTIONS

- Associate Editor of IEEE Transactions on Information Forensics and Security (IEEE TIFS)
- Associate Editor of International Journal of Information Security (IJIS), Springer
- Co-Affiliation and Supervision of PhD students at the University of Surrey, UK

Program Committee

- 21st International Conference on Applied Cryptography and Network Security (ACNS) 2023
- 18th ACM Symposium on Information, Computer, and Communications Security (ACM ASIACCS) 2023
- 28th European Symposium on Research in Computer Security (ESORICS)
- International Conference on Security for Information Technology and Communications (SECITC) 2023 (Chair)

Jun. Prof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

PUBLICATIONS

DARII, A., MOLL, M., NISTOR, M. S., PICKL, S., NOVAC, O., NOVAC, C. M., GORDAN, I. M., GORDAN, C. E.: Combination and Integration of Neuroevolution and Backpropagation Algorithms for Gaming Environment. 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). 2023.

EHRLICH, J., MOLL, M.; PICKL, S.: GTRF: Generalized Trade Reduction Framework for Double-auction Mechanisms. Operations Research Proceedings 2022. 2023.

MILANI, R., ARNOLD, J., MOLL, M., PICKL, S.: Expanding Reinforcement Learning Modeling Capabilities in Emergency Supply Distribution via Action Masking. Proceedings of the International Conference on Humanitarian Crisis Managment (KRISIS 2023). 2023.

MOLL, M., KARPUS, J., BAHRAMI, B.: Do Artificial Agents Reproduce Human Strategies in the Advisers' Game?. Operations Research Proceedings 2022. 2023.

MILANI, R., MOLL, M., PICKL, S.: Advances in Explainable Reinforcement Learning: An Intelligent Transportation Systems perspective. Explainable AI for Intelligent Transportation Systems. 2023.

MILANI, R., MOLL, M., PICKL, S.: Iterated Boxed Pigs Game: A Reinforcement Learning Approach. Operations Research Proceedings 2022. 2023.

MILANI, R., SAHIN, T., VON DANWITZ, M., MOLL, M., PICKL, S.: Automatic Concrete Bridge Crack Detection from Strain Measurements: a Preliminary Study. CRITIS 2022. Lecture Notes in Computer Science. 2023.

SCHMAUDER, C., KARPUS, J., MOLL, M., BAHRAMI, B., DEROY, O.: Algorithmic Nudging: The Need for an Interdisciplinary Oversight. Topoi 42, pp. 799–807. 2023.

RESEARCH PROJECTS

Digital workplace and human AI-assisted training through touch

Considering the importance of artificial assistance systems, the project investigates their inclusion in the training process. This is done from the perspective of human learning (cognitive science), machine learning (computer science) and by analyzing trust in AI partners (philosophy).

Funded by: Bavarian Research Institute for Digital Transformation (bidt)
Duration: 04/2022 – 03/2024

TEACHING

10361	**Operations Research**
14901	**Selected Chapters of Operations Research and Decision Theory**
29941	**Selected Chapters of Data-driven Optimization**
22942	**Quantum Machine Learning & Optimization**

FAIRS, CONFERENCES, SEMINARS

- Annual Conference of the Society for Operations Research in Germany, OR2023
- Workshop of the working group on "Simulation and Optimization of Complex Systems"
- 19th Cologne-Twente Workshop on Graphs and Combinatorial Optimization
- EU CSDP Innovation Day

ADDITIONAL FUNCTIONS

- Working Group Leader "Simulation and Optimization of Complex Systems", German Operations Research Society

Prof. Dr.
Eirini Ntoutsi

Open Source Intelligence

PUBLICATIONS

FABBRIZZI, S., ZHAO, X., KRASANAKIS, E., PAPADOPOULOS, S., NTOUTSI, E. (2023). Studying Bias in Visual Features Through the Lens of Optimal Transport. Data Mining and Knowledge Discovery, pp. 1–32.

GHODSI, S., NTOUTSI, E. (2023). Affinity Clustering Framework for Data Debiasing Using Pairwise Distribution Discrepancy. Proceedings of the 2nd European Workshop on Algorithmic Fairness. Winterthur, Switzerland, June 7–9, 2023. CEUR Workshop Proceedings. 3442.

GKOLEMIS, V., DALAMAGAS, T., NTOUTSI, E., DIOU, C. (2023). Regionally Additive Models Explainable-by-Design Models Minimizing Feature Interactions, XAI-uncertainty Workshop, co-located with ECML PKDD 2023.

GKOLEMIS, V., DALAMAGAS, T., NTOUTSI, E., DIOU, C. (2023). RHALE, Robust and Heterogeneity-aware Accumulated Local Effects, 26th European Conference on Artificial Intelligence (ECAI 2023).

IOSIFIDIS, V., PAPADOPOULOS, S., ROSENHAHN, B., NTOUTSI, E. (2023). AdaCC: Cumulative Cost-sensitive Boosting for Imbalanced Classification. Knowledge and Information Systems, 65(2), pp. 789–826.

LE QUY, T., FRIEGE, G, NTOUTSI, E. (2023). A Review of Clustering Models in Educational Data Science Toward Fairness-aware Learning. In: Peña-Ayala, Alejandro (Ed.). Educational Data Science: Essentials, Approaches, and Tendencies. Proactive Education Based on Empirical Big Data Evidence. Singapore. Springer Nature Singapore. pp. 43–94.

LE QUY, T., FRIEGE, G., NTOUTSI, E. (2023). Multi-fair Capacitated Students-Topics Grouping Problem. In Pacific-Asia Conference on Knowledge Discovery and Data Mining (pp. 507–519). Cham: Springer Nature Switzerland.

PANAGIOTOU, E., NTOUTSI, E. (2023). Learning Impartial Policies for Sequential Counterfactual Explanations Using Deep Reinforcement Learning, DynXAI Workshop co-located with ECML PKDD 2023.

PANAGIOTOU, E., QIAN, H., WYNANTS, M., KRIESE, A., MARX, S., NTOUTSI, E. (2023). Explainable AI-based Generation of Offshore Substructure Designs, ISOPE International Ocean and Polar Engineering Conference. The Society of Petroleum Engineers (SPE). S. ISOPE-I-23-045.

QIAN, H., PANAGIOTOU, E., MARX, S., NTOUTSI, E. (2023). Data-based Conceptual Design of Offshore Jackets Using a Self-Developed Database. ISOPE International Ocean and Polar Engineering Conference. The Society of Petroleum Engineers (SPE). S. ISOPE-I-23-154.

ROY, A., HORSTMANN, J., NTOUTSI, E. (2023). Multi-dimensional Discrimination in Law and Machine Learning: A Comparative Overview. In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, pp. 89–100.

RESEARCH PROJECTS

BIAS – Bias and Discrimination in Big Data and Algorithmic Processing. Philosophical Assessments, Legal Dimensions, and Technical Solutions

We provide philosophical analyses of the relevant concepts and principles in the context of AI (bias, discrimination, fairness), investigate their adequate reception in pertinent legal frameworks (data protection, consumer, competition, anti-discrimination law), and develop concrete technical solutions (debiasing strategies, discrimination detection procedures etc.).

Funded by: Volkswagen Foundation
Duration: 12/2018 – 05/2023

Hephaestus – Machine learning methods for adaptive process planning of 5-axis milling

The project aims to research a framework for a learning 5-axes compensation of shape errors in milling processes based on a process-parallel material removal simulation and sophisticated machine learning (ML) strategies. Moreover, we aim to investigate the ability of knowledge transfer between different workpiece geometries, milling tools and machine tools for an enhanced process planning.

Funded by: DFG
Duration: 04/2021 – 11/2024

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

MAMMoth concentrates on identifying and addressing (multi-)discrimination in AI systems concerning various protected attributes, encompassing both conventional tabular data and more intricate network and visual data. The developed solutions will be pilot tested in three relevant sectors of interest: a) finance/loan applications, b) identity verification systems, and c) academic evaluation.

Funded by: EU
Duration: 09/2022 – 08/2025

TEACHING

23191	**Artificial Intelligence**
23192	**Seminar Selected topics in Artificial Intelligence and Machine Learning**
23201	**Responsible Artificial Intelligence**
23211	**Machine Learning**
23212	**Machine Learning Lab**

FAIRS, CONFERENCES, SEMINARS

- Co-organizer of the BIAS workshop, co-located with ECML PKDD 2023.
- Keynote on Bias in AI Systems at IEEE ICCNS 2023
- Organization of the Workshop on Challenges and Opportunities of AI as part of the CODE-Jahrestagung 2023.
- Closing workshop for the Volkswagen Project Bias in Hannover, April 2023
- Participation at the Dagstuhl Dagstuhl seminar 23431 Network Attack Detection and Defense – AI-Powered Threats and Responses
- Invited talk on responsible AI at the Club of Greek Academics in Munich
- Participation in the Open Day at UniBw M, June 2023
- Co-organizer of the CODE colloquium (with Prof. Dr. Manulis)
- Leacture series on how machines learn and the ambivalences of AI, visit from Highly-gifted class of the Maria Theresia Gymnasium, November 2023h

ADDITIONAL FUCTIONS

- External advisory board for the new master AI in Society at TUM
- Member of the Scientific Network “Digital Bioethics”
- Reviewer for the European Commission
- Reviewer for the Swedish research council
- Reviewer for the Luxembourg national research fund

Program Committee

- DSAA 2023
- ECAI 2023
- ECML PKDD 2023

Prof. Dr. Stefan Pickl

Operations Research – Research Group COMTESSA

PUBLICATIONS

ALONSO VILLOTA, M., WILLKOMM, E., PICKL, S. (2023). Hybrid Threats to the European Union's Energy Sector: An Overview. In: Fathi, M., Zio, E., Pardalos, P.M. (Ed.). Handbook of Smart Energy Systems. Springer, Cham. https://doi.org/10.1007/978-3-030-72322-4_37-1

ZHARIKOVA, M., BARBEITO, G., PICKL, S. (2023). Reliability and Risk Analysis in Critical Infrastructure Protection. In: Ram, M.; Xing, L. (Ed.). Advances in Reliability Science. Reliability Modeling with Industry 4.0. Elsevier, 2023, pp. 35–43. https://doi.org/10.1016/B978-0-323-99204-6.00003-0

IFFLÄNDER, L., BUDER, T., LORETH, T., ALONSO VILLOTA, M., SCHMITZ, W., NEUBECKER, K.A., PICKL, S. (2023). Physical Attacks on the Railway System. CoRR, June 2023. https://doi.org/10.48550/arXiv.2306.00623

MILANI, R., MOLL, M., DE LEONE, R., PICKL, S. (2023). A Bayesian Network Approach to Explainable Reinforcement Learning with Distal Information. Sensors. 2023; 23(4): 2013. https://doi.org/10.3390/s23042013

TEACHING

10245	**Operations Research Lab – Decision Support I**
10252	**Selected Chapters of Operations Research Seminar 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**

ICE Lecture 2023

Intelligence Collection Europe
together with Gerhard Conrad and
Maximilian Moll
"Cyber and its Implications for Intelligence, Analysis and Decision Making"

FAIRS, CONFERENCES, SEMINARS

- CRITIS 2023 – 18th International Conference on Critical Information Infrastructures Security
- CTW 2023 – 19th Cologne Twente Workshop on Graphs and Combinatorial Optimization
- HOLM Seminar 2023 – "Quantum-Computing in Aviation, Logistics und Mobility"

PRIZES AND AWARDS

- NATO Excellence Award 2023 together with the STO Specialist Team SAS169

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

Prof. Dr. Daniel Slamanig

Cryptology

PUBLICATIONS

CRITES, E., KOHLWEISS, M., PRENEEL, B., SEDAGHAT, M., SLAMANIG, D.: Threshold Structure-preserving Signatures. Advances in Cryptology – ASIACRYPT 2023 – 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4–8, 2023, Springer.

GÖTH, C., RAMACHER, S., SLAMANIG, D., STRIECKS, C., TAIRI, E., ZIKULNIG, A.: Optimizing 0-RTT Key Exchange with Full Forward Security. 2023 ACM Cloud Computing Security Workshop - CCSW 2023, Copenhagen, Denmark, 26 November 2023, ACM.

MIR, O., BAUER, B., GRIFFY, S., LYSYANSKAYA, A., SLAMANIG, D.: Aggregate Signatures with Versatile Randomization and Issuer-hiding Multi-authority Anonymous Credentials. 2023 ACM SIGSAC Conference on Computer and Communications Security – CCS 2023, Copenhagen, Denmark, November 26–30, 2023, ACM.

MIR, O., SLAMANIG, D., BAUER, B., MAYRHOFER, R.: Practical Delegatable Anonymous Credentials From Equivalence Class Signatures. Proc. Priv. Enhancing Technol. 2023.3.

MIR, O., SLAMANIG, D., MAYRHOFER, R.: Threshold Delegatable Anonymous Credentials with Controlled and Fine-grained Delegation. IEEE Transactions on Dependable and Secure Computing, 2023.

RÖSLER, P., SLAMANIG, D., STRIECKS, C.: Unique-path Identity-based Encryption with Applications to Strongly Secure Messaging. Advances in Cryptology – EUROCRYPT 2023 – 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Springer.

SLAMANIG, D., STRIECKS C.: Revisiting Updatable Encryption: Controlled Forward Security, Constructions and a Puncturable Perspective. Theory of Cryptography – 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 – December 2, 2023, Springer.

FAIRS, CONFERENCES, SEMINARS

- 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2023 (Session Chair "Signature Schemes").

PRIZES AND AWARDS

- Top Reviewer Award at the 30th ACM SIGSAC Conference on Computer and Communications Security (CCS 2023).

ADDITIONAL FUNCTIONS

- Reviewer for the European Commission
- Academic Editor for IET Information Security

Program Committee

- 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2023)
- 30th Annual ACM Conference on Computer and Communications Security (ACM CCS 2023)
- 28th Australasian Conference on Information Security and Privacy (ACISP 2023)
- 26th Information Security Conference (ISC 2023)
- 17th International Conference on Provable and Practical Security (ProvSec 2023)
- The 26th Annual International Conference on Information Security and Cryptology (ICISC 2023)
- 38th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2023)
- 18th International Workshop on Security (IWSEC 2023)
- 10th ACM Asia Public-Key Cryptography Workshop (APKC 2023)
- 23rd Central European Conference on Cryptology (CECC 2023)

Prof. Dr. Gunnar Teege

Formal Methods for Securing Things (FOMSET)

RESEARCH PROJECTS

MiKscHA: Microkernel for static and cloud based high security applications

The project evaluates state-of-the-art methods for the highly secure operation of microkernel-based applications. The focus is on the secure start of the system. The methods used shall be sufficient to support a successful system certification.

Funded by: Airbus CyberSecurity
Duration: 01/2021 – 12/2023

SW_GruVe: Extending the Basiscs of formal verification for software and its applications.

The goal is to make formal verification amenable to the practical application in software development. The focus is hardware related software in the C programming language as part of operating systems. The verification uses the programming language Cogent and the proof assistant Isabelle.

Funded by: Bavarian Ministry of Economic Affairs, Regional Development and Energy (StMWi)
Duration: 10/2020 – 09/2023

TEACHING

1016	**Introduction to Computer Networks**
1016	**Introduction to Operating Systems**
1026	**Distributed Systems**
5505	**Operating Systems Security**

ADDITIONAL FUNCTIONS

- Member of the examinations board for Master Cybersecurity
- Member of the study program commission for Master Cybersecurity
- Member of the examinations board for Computer Science
- Member of the examinations board for Information Systems

Prof. Dr. Arno Wacker

Privacy and Compliance

PUBLICATIONS

HECK, H., WACKER, A.: Disjoint Lookups in Kademlia for Random IDs. 2023 IEEE International Conference on Autonomic Computing and Self-organizing Systems Companion (ACSOS-C), Toronto, ON, Canada, 2023, pp. 47–52, doi: 10.1109/ACSOS-C58168.2023.00035.

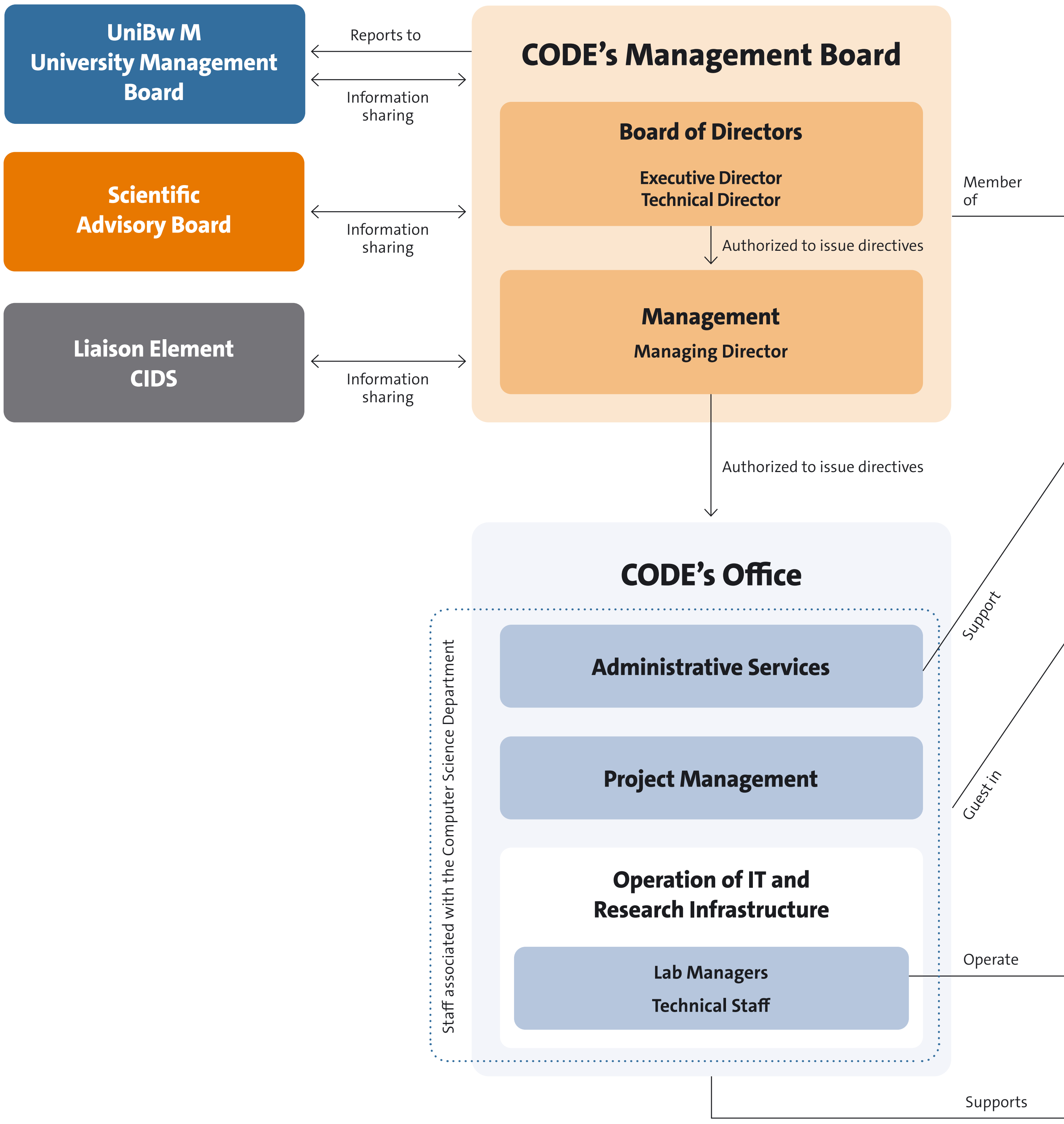
TEACHING

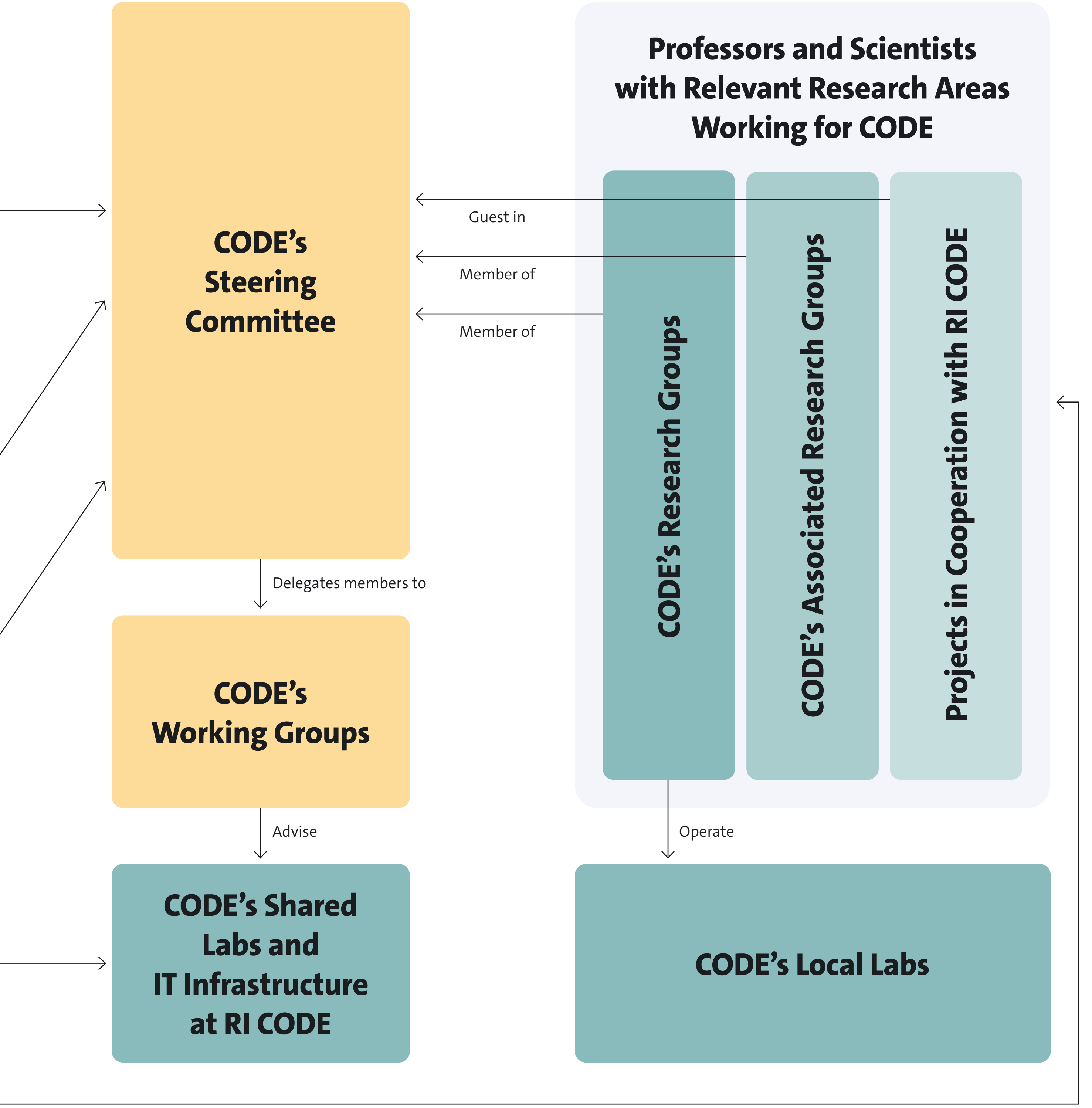
3480	**Secure Networks and Protocols**
55011	**Vulnerabilities and Attack Vectors Seminar**
55041	**Data Privacy**
55042	**Privacy Enhancing Technologies**
55061	**Introduction to Cryptography**
55091	**Penetration Testing**
55093	**Penetration Testing Lab**

ADDITIONAL EVENTS

- March 2, 2023, Lecture “From data-at-rest to domain-at-risk”
  - Presentation at the 1st IT-Grundschutz-Tag 2023 of the BSI. Prof. Dr. Arno Wacker and Christoph Ruhl used practical examples to demonstrate the strengths and limitations of hard disk encryption.
- March 30–31, 2023, CrypTool-Symposium
  - The CrypTool Symposium took place on the occasion of the 25th anniversary of the CrypTool project. The official transfer of the management of CryptTool from Prof. Dr. Esslinger to Prof. Dr. Wacker, and thus to the University of Bundeswehr Munich, was particularly important for our professorship.
- June 20–22, 2023, HistoCrypt conference at the Deutsches Museum
  - This year, the HistoCrypt conference took place at the Deutsches Museum under the responsibility of Prof. Dr. Wacker.
- July 3, 2023, Lecture “You’re Being Watched – Tricks und Tools der Hacker”
  - Prof. Dr. Arno Wacker and Dr. Olga Kieselmann gave a live demonstration of the dangers lurking for personal data in everyday life.
- Oct. 20, 2023, Schuelerkrypto (Crpyto for Students) 2023 at the Youth Science Club
  - Prof. Dr. Arno Wacker gave an introductory lecture on “Cryptography” to members of the Youth Science Club at the Munich Observatory and was available to answer a large number of questions afterwards.
- Nov. 11, 2023, Lecture “Web(in)security”
  - Prof. Dr. Arno Wacker provided a quick but in-depth insight into the diverse attack possibilities on web applications at the IT Security Day 2023 in Kassel.

Organization of RI CODE




Professors and Scientists with Relevant Research Areas Working for CODE
CODE's Steering Committee
Guest in
Member of
Member of
CODE's Research Groups
CODE's Associated Research Groups
Projects in Cooperation with RI CODE
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 22
81739 Munich
Germany

@ code@unibw.de

☎ +49 89 6004 7300

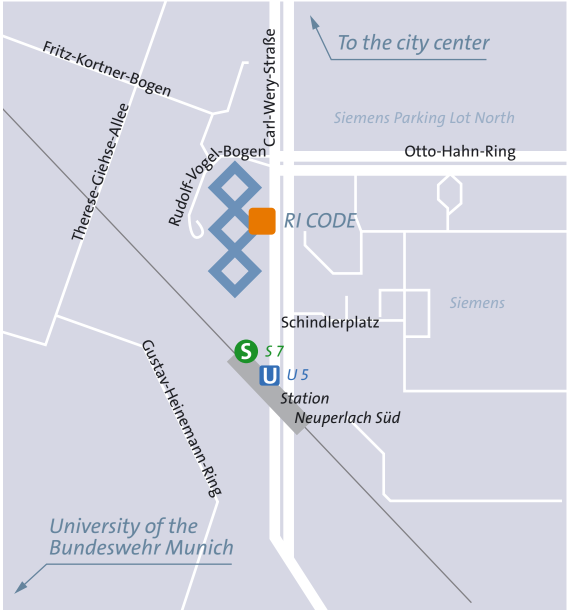
www.unibw.de/code

X (prev. Twitter): @FI_CODE

LinkedIn: Forschungsinstitut Cyber Defence (CODE)

YouTube: Forschungsinstitut Cyber Defence

Location Map



Editorial Information

PUBLISHER

Prof. Dr. Wolfgang Hommel,
Prof. Dr. Michaela Geierhos,
Marcus Knüpfer,
Benjamin Bellgrau

Research Institute CODE
University of the Bundeswehr Munich
Carl-Wery-Str. 22
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

PROFESSORS AT RI CODE

Prof. Dr. Florian Alt,
Professor for Usable Security and Privacy

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,
Professor for Machine Learning

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

Prof. Dr. Wolfgang Hommel,
Professor for Software and Data Security

Prof. Dr.-Ing. Mark Manulis,
Professor for Privacy

Prof. Dr.-Ing. Helmut Mayer,
Professor for Visual Computing

Jun. Prof. Dr. Maximilian Moll,
Junior Professor for Operations Research – Prescriptive Analytics

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

Prof. Dr. Stefan Pickl,
Professor for Operations Research

Prof. Dr. Daniel Slamanig,
Professor for Cryptology

Prof. Dr. Gunnar Teege,
Professor for Distributed Systems

Prof. Dr. Arno Wacker,
Professor for Data Privacy and Compliance

MEMBERS OF THE ADVISORY BOARD (IN 2023)

From the Department for Computer Science at the University of the Bundeswehr Munich:

Prof. Klaus Buchenrieder, Ph.D.

Prof. Dr. Ulrike Lechner

Prof. Dr.-Ing. Helmut Mayer

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

Other Members

Dr. Norbert Gaus,
Executive Vice President of Siemens AG

Prof. Dr. Johann Pongratz,
TU Dortmund

Wolfgang Sachs,
Head of Division CIT I.2, Federal Ministry of Defense

Dr. Ralf Wintergerst,
Chairman of the Management Board of Giesecke+Devrient

EDITING AND COORDINATION

Benjamin Bellgrau, M. Sc.,
Public Relations Officer

ART DIRECTION

Tausendblauwerk Design Agency
Michael Berwanger

www.tausendblauwerk.de

PROOFREADING

Dr. Michelle Ruth Büscher,
Technical Translator/Editor

PRINTED BY

druckhaus köthen

https://koethen.de

REGULATIONS

Editorial deadline: March 2024

Title illustration: iStock / dem10

ISBN: 978-3-943207-87-3 | ISSN: 2748-9485

Also published as an electronic publication
(ISBN: 978-3-943207-88-0 | ISSN: 2748-9507)
as well as in German language
(ISBN: 978-3-943207-85-9 | ISSN: 2748-8780).

der Bundeswehr
Universität München

RI
CODE
Research Institute
Cyber Defence
Universität der Bundeswehr München