Zeitschrift für Außen- und Sicherheitspolitik
https://doi.org/10.1007/s12399-023-00974-4

BERICHT

CODE-Jahrestagung 2023: Zehn Jahre Forschung und Vernetzung im Bereich Cybersicherheit

Wolfgang Hommel · Michaela Geierhos · Marcus Knüpfer · Benjamin Bellgrau · Ulrike Schreiber · Julius Zahn

Angenommen: 23. November 2023

Mit der zunehmenden Vernetzung und den neuen Technologien in der IT-Branche sowie den veränderten Bedrohungen in der Sicherheitspolitik wachsen auch die Herausforderungen in der Cybersicherheit. Diesen Bereich zu erforschen und den Austausch zwischen Stakeholdern zu fördern, hat sich CODE vor zehn Jahren auf die Fahnen geschrieben. Zehn Jahre CODE – zehn Jahre Spitzenforschung in den Bereichen Cybersicherheit, Künstliche Intelligenz und Quantentechnologien. Ganz im Zeichen dieses Jubiläums stand die Jahrestagung des Forschungsinstituts Cyber Defence und Smart Data (FI CODE) am 11. und 12. Juli 2023. Mehr als 400 Teilnehmer*innen aus Militär, Industrie, Wissenschaft und Behörden, darunter auch internationale Gäste, trafen sich auf dem Campus der Universität der Bundeswehr München (UniBw M) in Neubiberg. Hochrangige Vertreter*innen würdigten in ihren Beiträgen die Arbeit von CODE – nicht nur als zentrale Forschungseinrichtung, sondern auch als Anlaufstelle und Vermittler in Cybersicherheitsfragen.

Den Auftakt des ersten Veranstaltungstages machte die Präsidentin der Universität der Bundeswehr München, Professorin Eva-Maria Kern. In ihrer Begrüßungsrede betonte sie die Bedeutung des Themas Sicherheit, das durch den Krieg in der Ukraine und die damit verbundene Zeitenwende in Deutschland wieder an gesellschaftlicher Relevanz gewonnen habe. Die Erfolgsgeschichte von CODE zeige, wie wichtig gerade im Bereich der Cybersicherheit die Zusammenarbeit zwischen der Universität, Behörden und der Wirtschaft sei. „Diese Zusammenarbeit zwischen Forschenden und Bedarfsträgern ist entscheidend für das Vorankommen, um sinnvolle Lösungen zu erarbeiten." Längst sei die Universität der Bundeswehr München neben einer Ausbildungsstätte für das Offizierskorps der Bundeswehr auch eine strategische

✉ Julius Zahn
Forschungsinstitut CODE, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, 85579 Neubiberg, Deutschland
E-Mail: julius.zahn@unibw.de

Published online: 21 December 2023

Ressource für das Bundesministerium der Verteidigung (BMVg) im Kontext der Forschung. Diese beiden Dimensionen vereine auch das Forschungsinstitut CODE und helfe damit Deutschland, die Herausforderungen unserer Zeit zu meistern. Mit viel Engagement sei es CODE gelungen, vor zehn Jahren seiner Zeit voraus und in der Folge mit seiner Forschungsarbeit heute am Puls der Zeit zu sein.

Ähnlich äußerte sich Siemtje Möller, Parlamentarische Staatssekretärin beim Bundesminister der Verteidigung, in ihrer Videobotschaft. Angriffe im Cyber- und Informationsraum seien keine abstrakten Zukunftsszenarien mehr. „Moderne Kriege beginnen weit bevor die ersten Panzer die Grenze überqueren". Die Einsatzbereitschaft und Wirkungsüberlegenheit der Bundeswehr hänge heute „dimensionsübergreifend" vom Cyberraum ab. In diesem Zusammenhang lobte die Staatssekretärin den von CODE gepflegten Austausch mit zivilen und militärischen Akteuren, der zu einem Wissenstransfer beitrage und durch den die Resilienz von Bundeswehr und Gesellschaft gestärkt werde. Darüber hinaus betonte Möller die Bedeutung der Grundlagenforschung am FI CODE, aber auch die praxisnahe Aus- und Weiterbildung von Fach- und Führungskräften, die hier stattfinde. Sie resümierte: „CODE trägt entscheidend zur Digitalisierung der Streitkräfte bei und sorgt dafür, dass wir nicht nur auf dem Laufenden bleiben, sondern ‚ahead of the curve' kommen."

Ganz im Sinne des Tagungsmottos „10 Jahre CODE" ließ der Leitende Direktor des Forschungsinstituts CODE, Professor Wolfgang Hommel, in seinem Vortrag die vergangene Dekade Revue passieren. In einer kurzweiligen Zeitreise durch die letzten zehn Jahre gab er dem Publikum einen Einblick in die Geschichte von CODE. 2013 als viertes Forschungszentrum an der UniBw M gegründet und 2017 zum Forschungsinstitut ausgebaut, arbeiten heute mehr als 130 Mitarbeiter*innen in über 40 Projekten an Zukunftsthemen. Trotz zuletzt rückläufiger Anfängerzahlen in den Bachelorstudiengängen Informatik und Wirtschaftsinformatik an der UniBw M erfreut sich der 2018 gestartete Masterstudiengang Cyber-Sicherheit (MCYB) weiterhin eines stetigen Zuwachses. Die 96 neu geschaffenen Lehrveranstaltungen im Bereich MCYB bieten zudem ein breites Spektrum an Wahl- und Spezialisierungsmöglichkeiten für die Studierenden. Stolz zeigte sich Professor Hommel auch über die praxisnahe Ausbildungsumgebung der *Cyber Range*, in der Fachkräfte der Bundeswehr, der Cyber-Reserve und zunehmend auch von Behörden aus- und weitergebildet werden. Zum Abschluss seines Vortrags hob der Leitende Direktor das Thema Kooperation und Vernetzung hervor. CODE vermittelt seit Jahren erfolgreich zwischen Bundeswehr, Behörden, Industrie sowie Forschung und Wissenschaft und wird diese Aufgabe auch in Zukunft wahrnehmen.

In seiner anschließenden *Keynote* ging Vizeadmiral Thomas Daum, Inspekteur Cyber- und Informationsraum (CIR), unter anderem auf die immer schnelleren Entwicklungen im Bereich Künstliche Intelligenz ein. Die Qualität maschinell erstellter Texte sei kaum noch von der Qualität menschlicher Texte zu unterscheiden. Dies untermauerte er mit einem eindrucksvollen Beispiel: Der Einstieg in seine Rede wurde komplett mit ChatGPT verfasst, wie Vizeadmiral Daum später erläuterte. Seit der Aufstellung des Kommandos Cyber- und Informationsraum im Jahr 2017 sei das FI CODE ein „unerlässlicher Partner" in der Forschungs- und Entwicklungsarbeit sowie im Expertenaustausch und ganz besonders in der Aus- und Weiterbildung. „Die

Technologie der Zukunft wird bei CODE zur Technologie der Gegenwart.“ Die Zahl der laufenden Projekte zeige, dass bei CODE Innovation geschaffen werde. Begeistert zeigte sich der Inspekteur von der Kooperation mit IBM im Bereich Quantencomputing. Der Zugriff auf das hochmoderne Quantencomputersystem ermögliche es der Bundeswehr seit 2018, Erfahrungen und Erkenntnisse mit dieser Technologie zu sammeln und darauf aufbauend zeitnah marktfähige Lösungen im Bereich der Verschlüsselungstechnik und der Datenanalyse zu entwickeln. Dies ist nur eines von vielen Projekten, mit welchen CODE einen Baustein für die Sicherheitsarchitektur in Europa liefert. Insofern schloss sich Daum der Aussage der ehemaligen Bundesverteidigungsministerin Kramp-Karrenbauer an: „CODE ist ein ‚golden Nugget‘ nicht nur für den Organisationsbereich CIR, sondern für die gesamte Sicherheit Deutschlands und seiner Bündnispartner.“

Der Vortrag von Barbara Kluge vom Bundesministerium des Innern und für Heimat (BMI) verdeutlichte, dass gerade die Cybersicherheitsforschung nur gemeinsam erfolgreich sein kann. Eine enge und vertrauensvolle Zusammenarbeit sei der Erfolgsfaktor für ein Gelingen – „Nur gemeinsam sind wir stark“. Sie hob besonders die enge Kooperation zwischen dem BMI und dem FI CODE hervor: „Gemeinsam Fachkräfte ausbilden [...], Synergieeffekte erkennen und Bedrohungen [...] in den Griff bekommen“, so Kluge. CODE habe sich in den vergangenen zehn Jahren als fester Bestandteil der Cybersicherheitslandschaft etabliert und maßgeblich dazu beigetragen, das Vertrauen und die Zusammenarbeit in der Forschung zu stärken. „Cybersicherheit ohne Forschung kann und wird nicht funktionieren. Wir haben gelernt, wie schnell die Fortschritte sind auf der dunklen Seite [...] – die Guten müssen Schritt halten.“ Für die Vielzahl an herausfordernden Themen sind echte Expert*innen wichtig. Diese Fachleute werden bei CODE ausgebildet, um ihr Know-how später auch im BMI einzubringen und tatkräftige Unterstützung zu leisten. „Indem wir Wissen und Erfahrungen teilen, können wir unsere Schutzmaßnahmen effektiver gestalten und unsere Infrastrukturen resilienter machen.“

Nach einer kurzen Kaffeepause wurde das Programm mit Vorträgen von Bernd Schlömer, Staatssekretär im Ministerium für Infrastruktur und Digitales des Landes Sachsen-Anhalt und Beauftragter der Landesregierung für die Informationstechnik, und Wilfried Karl, Präsident Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) fortgesetzt.

Schlömer beleuchtete in seinem Vortrag den aktuellen Stand der Digitalisierung und Informationssicherheit im Spannungsfeld zwischen Land und Kommunen. Wie eine erfolgreiche Digitalisierung von Verwaltungsdienstleistungen aussehen kann, zeigte Schlömer am Beispiel der automatisierten Plattform für die 200-Euro-Einmalzahlung an Schüler*innen und Studierende, die ohne Eingreifen von Sachbearbeiter*innen auskommt. Den Grund für das häufige Scheitern von Digitalisierungsprojekten in der Verwaltung sieht der Staatssekretär in der fehlenden Projekt- und Prozessmanagement-Expertise in der öffentlichen Verwaltung. Abhilfe sollen zukünftig Digitallotsen*innen schaffen, welche die Verwaltung beim Projektmanagement unterstützen. Durch die verpflichtende Umsetzung der NIS2-Richtlinie soll ein Grundschutz für IT-Systeme der öffentlichen Verwaltung und kritischen Infrastrukturen bis auf die kommunale Ebene gewährleistet werden. Im Bereich der

Cyber- und Informationssicherheit müsse viel stärker als bisher ebenenübergreifend zwischen Land und Bund zusammengearbeitet werden, mahnte Schlömer an.

Auch ZITiS-Präsident Wilfried Karl griff den Aspekt der Zusammenarbeit auf und bezeichnete Kooperation und Wissen als „Fundament der Cybersicherheit". Ob Hass und Hetze im Internet, die Verbreitung von Fake News und Deepfakes oder der zunehmende Online-Drogenhandel – den vielfältigen Herausforderungen durch neue Technologien könne nur mit Kooperation und Wissen begegnet werden. Diese Kooperation in der Forschung sei mit CODE in den vergangenen Jahren etabliert worden und nach wie vor essentiell für den Wissensaufbau. Dies allein reiche aber nicht aus. So fehle es derzeit vor allem an IT-Fachkräften, die die technischen Innovationen umsetzen. Er verwies dabei auf die seit Jahren rückläufigen Studienanfänger*innenzahlen im IT-Bereich. Erschwerend komme hinzu, dass viele nationale und supranationale Behörden um dieselben Fachkräfte werben. Zur Lösung dieses Problems und Steigerung der Effizienz schlug Karl eine stärkere Bündelung von Personalressourcen und Wissen vor.

Kurz vor der Mittagspause folgte ein weiteres Highlight. IBM und die UniBw M verlängerten ihre Partnerschaft im Bereich Quantencomputing um weitere fünf Jahre. In einer feierlichen Zeremonie wurde der Vertrag unterzeichnet. Als Quantum Innovation Center eröffnen sich insbesondere für das FI CODE damit weiterhin Möglichkeiten der Forschung und Lehre in diesem zukunftsträchtigen Bereich. Auch hier ist Kooperation der Schlüssel zum Erfolg: Als Beteiligte in mehreren regionalen und internationalen Quantum-Netzwerken profitieren die UniBw M und CODE von starken Partnerschaften, guter Vernetzung und offenem Informationsaustausch.

Am Nachmittag folgten weitere Vorträge, unter anderem von den CODE-Professor*innen Professor Harald Baier und Professorin Eirini Ntoutsi, die in ihren Beiträgen zu Digitaler Forensik bzw. *Responsible AI* Einblicke in die aktuelle Forschung am FI CODE gaben. Ramon Mörl, Geschäftsführer der itWatch GmbH sprach über „Distributed Ledger, Blockchain als Treiber für eine praktische Lösung zum Management von Digitaler Souveränität". Anschließend stellte Sven Meyer-Ottens vom Bundesnachrichtendienst (BND) den Innovationshub des BND vor. Einen Rückblick und Ausblick auf IT-Sicherheit gab Dirk Häger vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bevor Professor Rainer Blatt, Wissenschaftlicher Direktor am Institut für Quantenoptik und Quanteninformation (IQOQI) der Österreichischen Akademie der Wissenschaften (ÖAW) mit seinem Beitrag zu „Quantentechnologien für das Informationszeitalter" die Vortragsreihe des Nachmittags abschloss.

Nach dem Anschnitt des CODE-Geburtstagskuchens durch die Technische Direktorin des FI CODE, Professorin Michaela Geierhos, stand im letzten Veranstaltungsblock des Nachmittags das Thema *Software-defined Defence* im Fokus der Betrachtungen. In seinem Impulsvortrag ging Michael Kiefer von Dassault Systems Deutschland auf die Bedeutung des Themas ein: „Software-defined Defence verändert die Art, wie Systeme entwickelt und eingesetzt werden". Zukünftig bestimmt die Software den Funktionsumfang der Hardware, so die Vision. Eine vereinfachte Steuerung und Überwachung sowie eine bessere Vernetzung der Waffensysteme untereinander sollen zukünftig zu einer Effizienzsteigerung des Personal- und Materialeinsatzes bei gleichzeitig verbessertem Schutz beitragen. Um nun bei der

Umsetzung von *Software-defined Defence* voranzugehen, brauche es neben finanziellen Mitteln auch „das richtige digitale Mindset, sowohl bei Herstellern und Politik als auch bei Beschaffern und Nutzern", so Kiefer. Bereits frühzeitig müsse auch das Thema Cybersicherheit mitgedacht werden. Bei der notwendigen strukturierten Planung und Umsetzung könne die Bundeswehr auf das Know-how des Cyber Innovation Hub, der Agentur für Innovation in der Cybersicherheit (Cyberagentur) und des FI CODE zurückgreifen.

Im Anschluss diskutierte Jens Ohlig vom Tagesspiegel Background zusammen mit Vertreter*innen aus Militär, Industrie und Interessenverbänden im Rahmen einer Paneldiskussion über die Potenziale und Risiken von *Software-defined Defence*. Zu Gast waren Karen Florschütz, Executive Vice-President Connected Intelligence bei Airbus Defence and Space, Markus Lehmann, Leiter Defence bei der Deutsche Telekom Geschäftskunden GmbH, Peter Obermark, Director Governmental Affairs bei der blackned GmbH sowie Kapitän zur See Daniel Prenzel, Referent Software Defined Defence in der Abteilung CIT I 3 im BMVg und Professor Stefan Brunthaler, Professor für Systemsicherheit am FI CODE. Den Chancen, mit technologischen Neuerungen Schritt zu halten und diese schnellstmöglich in der Truppe zur Anwendung zu bringen, stünden ebenso Risiken gegenüber. Dabei war insbesondere der Aspekt der Cybersicherheit Gegenstand der Diskussion. Es brauche vor allem sichere und verlässliche Daten, auf deren Grundlage beispielsweise KI-Systeme die Soldat*innen besser bei der Auftragserfüllung unterstützen könnten. Professor Brunthaler merkte an: „Letztendlich entscheidet auch der Aspekt der Cybersecurity über den Erfolg von Software-defined Defence". Forschung und Industrie müssten hier Hand in Hand arbeiten, um Probleme, wie etwa die unbemerkte Fälschung von Daten, zu lösen. *Software-defined Defence* als Leitprinzip für die zukünftige Beschaffung trage „maßgeblich zur Digitalisierung der Streitkräfte bei und damit auch zu einer höheren Durchsetzungsfähigkeit auf dem digitalen Gefechtsfeld", so Kapitän zur See Prenzel. Markus Lehmann resümierte, dass *Software-defined Defence* kein Trend sei, „aktuell gibt es keine Alternative".

Den Abschluss des ereignisreichen ersten Veranstaltungstages bildete ein *Social Event*, in dessen Rahmen der Bayerische Staatsminister Florian Herrmann eine *Dinner Speech* hielt. In seiner Rede sprach Herrmann unter anderem über die zunehmende Bedeutung von Cybersicherheitsfragen und lobte in diesem Zusammenhang insbesondere die Arbeit des FI CODE: „Das Forschungsinstitut CODE ist ein Aushängeschild der Bundeswehr in Bayern. Seit 2013 ist CODE das perfekte Beispiel, wie gute, vernetzte Zusammenarbeit im Bereich Cyber-Security funktioniert. [...] Verteidigung ist immer eine Teamaufgabe. Wir setzen auch weiterhin auf die enge Zusammenarbeit mit CODE, die mit ihrer exzellenten Forschungsarbeit entscheidend zur Sicherheit im digitalen Raum beitragen."

Tag zwei der *CODE-Jahrestagung* am 12. Juli begann nach der Begrüßung durch Professorin Michaela Geierhos mit zwei *Keynotes*. Brigadegeneral Armin Fleischmann, Unterabteilungsleiter Cyber-/Informationstechnik I des BMVg, griff das Thema *Software-defined Defence* vom Vortag noch einmal auf und verdeutlichte, welche Vorteile, aber auch welche Herausforderungen eine größere Fokussierung auf die Software bei der Fähigkeitsentwicklung mit sich bringt. In einer zweiten *Key-*

note unterstrich Professor Achim Walter von der Universität Kiel die Wichtigkeit von *Awareness* und aktiven Rahmenbedingungen, um Innovation bestmöglich zu fördern und „zum Leben zu erwecken“. Der Vortrag war thematisch ein passender Vorgriff auf den Nachmittag.

Der weitere Vormittag bot die Möglichkeit für tiefgreifende Diskussionen und Vorträge: In den fünf parallel durchgeführten Workshops konnten sich die Teilnehmenden unter anderem über Cyber-Range-Trainings im Kontext Kritischer Infrastrukturen sowie den Herausforderungen und Chancen der Künstlichen Intelligenz informieren oder sich mit Quantentechnologien und Drohnen-Forensik beschäftigen. Im Workshop zu Fördermaßnahmen im Bereich Cybersicherheit in den EU-Förderprogrammen „Horizont Europa“ und „Digitales Europa“ konnten die Teilnehmenden zudem mehr zu den Chancen und Beteiligungsregeln erfahren sowie Erfahrungswerte austauschen.

Auf der in Zusammenarbeit mit dem BMVg ausgerichteten Innovationstagung Cyber- und Informationstechnik wurden am Nachmittag vorab eingereichte Ideen vorgestellt. In seinem einleitenden Vortrag erläuterte Brigadegeneral Fleischmann die Zielsetzung. Seit der erstmaligen Durchführung der Innovationstagung 2018 ist das Ziel, neuartige IT-Innovationen aus universitären und außeruniversitären Forschungseinrichtungen sowie der Wirtschaft zu identifizieren, die besonders im Geschäftsbereich des BMVg Verwendung finden könnten.

Der mit 15.000 € dotierte erste Platz ging in diesem Jahr an Michael Kissner von der Akhetonics GmbH, der die Jury und das Publikum mit einem rein-photonischen, universellen Hochleistungsprozessor für homomorph verschlüsselte Daten überzeugen konnte. Platz zwei und 10.000 € Preisgeld sicherte sich Professor Michael Schmitt von der UniBw M und seiner Idee einer sensor- und blickwinkel-unabhängigen Veränderungsdetektion in Satellitenbildern. Über Rang drei konnte sich Jakob Vanhoefer von der LightningPose GmbH freuen. Die von ihm vorgestellte Vision einer App für die KI-gestützte Echtzeit-Analyse und -Korrektur von Körperhaltungen wurde mit einem Preisgeld von 5000 € prämiert. Zudem erhalten alle Finalisten der Innovationstagung die Möglichkeit, ihre Ideen den ausgewählten Zielgruppen innerhalb der Bundeswehr noch einmal im Detail zu erläutern und vorzustellen.

Die Jahrestagung endete mit dem *Wrap-up* und Schlusswort von Professorin Michaela Geierhos. Sie dankte allen Teilnehmer*innen für ihren Besuch und ganz besonders denjenigen, die in unterschiedlichster Form zur Jubiläumstagung beigetragen haben. Mit dem 9. und 10. Juli 2024 steht bereits der Termin für die nächste CODE-Jahrestagung fest.

Funding Open Access funding enabled and organized by Projekt DEAL.