

Gemeinsam mit KI gegen neue Cyberbedrohungen: Ein Bericht zur CODE-Jahrestagung 2024

Wolfgang Hommel  · Michaela Geierhos  · Marcus Knüpfer · Benjamin Bellgrau

Online publiziert: 22. April 2025
© The Author(s) 2025

1 Einleitung

Bei der CODE-Jahrestagung trafen sich am 10. und 11. Juli 2024 über 500 Teilnehmer*innen aus Wissenschaft, Behörden, Industrie und Militär auf dem Campus der Universität der Bundeswehr München (UniBw M). Unter dem Leitthema *Gemeinsam mit KI gegen neue Cyberbedrohungen* gab es Vorträge, Keynotes, Paneldiskussionen und Workshops von und mit hochkarätigen Expert*innen. In Kooperation mit dem Bundesministerium der Verteidigung (BMVg) fand zudem die Innovationstagung Cyber/IT statt, bei der auch in diesem Jahr wieder zahlreiche Erfindungen und Ideen präsentiert wurden, die zuvor von einer Fachjury gesichtet und als potenziell wertvoll für die Bundeswehr eingestuft wurden.

2 Die Zukunft liegt in der Zusammenarbeit von Menschen und KI

Der erste Tag begann mit der Begrüßung durch den Vizepräsidenten der UniBw M, Professor Uwe M. Borghoff und Professorin Michaela Geierhos, Technische Direktorin des Forschungsinstituts Cyber Defence und Smart Data (CODE). In ihrem

Prof. Dr. Wolfgang Hommel · Prof. Dr. Michaela Geierhos · Marcus Knüpfer · ✉ Benjamin Bellgrau
Forschungsinstitut CODE, Universität der Bundeswehr München,
Werner-Heisenberg-Weg 39, 85579 Neubiberg, Deutschland
E-Mail: benjamin.bellgrau@unibw.de

Prof. Dr. Wolfgang Hommel
E-Mail: wolfgang.hommel@unibw.de

Prof. Dr. Michaela Geierhos
E-Mail: michaela.geierhos@unibw.de

Marcus Knüpfer
E-Mail: marcus.knuepfer@unibw.de

Eröffnungsvortrag ging Geierhos auf die zunehmende Leistungsfähigkeit von auf Künstlicher Intelligenz (KI) basierender Anwendungen und Dienste ein, die den Menschen bei immer mehr Aufgaben unterstützen oder teilweise sogar ersetzen. Gleichzeitig warnte sie vor den Gefahren und Risiken, die mit dem Einsatz von KI verbunden sind. Sie plädierte dafür, „KI nicht zu verteufeln, sondern zu unseren Bedingungen nutzbar zu machen“, denn letztlich liege die Zukunft in der Zusammenarbeit von Menschen und KI im Kampf gegen Cyber-Bedrohungen. Im Anschluss folgte die Keynote von Brigadegeneral Michael Volkmer. Der Kommandeur des Zentrums für Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw) berichtete unter anderem über die aktuellen Bestrebungen des ZDigBw zur Bereitstellung einer IT-Basisinfrastruktur für die Digitalisierung der Streitkräfte bis 2029. Angesichts der Bedrohungslage benötige die Truppe bereits in den nächsten Jahren „praktikable, robuste und im Gefecht nutzbare digitale Lösungen“, so Volkmer. Dabei schaffe vor allem die Geschwindigkeit, mit der marktverfügbare Technologien, wie etwa Cloud Computing, KI oder Drohnen, der Truppe zur Verfügung gestellt werden können, entscheidende operativ-taktische Vorteile. In diesem Zusammenhang lobte der Brigadegeneral die Digitalisierungsplattform, die unter anderem mehr Agilität und Geschwindigkeit bei der Planung und Realisierung von IT in der Bundeswehr ermögliche. Bis 2029 sei die Realisierung von rund 30 Großprojekten mit einem Gesamtvolumen von circa 20 Mrd. € aus dem Sondervermögen der Bundeswehr geplant, um eine Basisinfrastruktur zu schaffen, die auch die Bereitstellung von KI-Diensten beinhalte. Norbert Pohlmann, Professor für Informationssicherheit sowie Geschäftsführer des Instituts für Internet-Sicherheit (if(is)) an der Westfälischen Hochschule Gelsenkirchen, beleuchtete in seinem Vortrag das Thema „IT-Sicherheit und Künstliche Intelligenz“. Nach einer Einführung zeigte er nicht nur auf, wie KI zur Verbesserung der IT-Sicherheit genutzt werden kann, sondern umgekehrt auch, wie IT-Sicherheit für KI genutzt werden kann. „KI braucht Vertrauen: Nicht nur die Firmen, die KI-Technologie anbieten, sondern auch die eingesetzten Technologien selbst müssen vertrauenswürdig sein.“ Dazu müsse sich auch das Kräfteverhältnis zwischen Angreifern und Verteidigern ändern. Hierfür müssten die Verteidiger künftig sicherheitsrelevante Daten untereinander austauschen und bei der Umsetzung von KI stärker kooperieren.

Mit drei Vorträgen zum Thema KI wurde das Nachmittagsprogramm nach den Eröffnungsvorträgen und einer Pause fortgesetzt. Professor Christian Hummert, Forschungsdirektor und Geschäftsführer der Cyberagentur, knüpfte mit seinem Vortrag „Sicherheit für KI“ an das Thema des Vormittags an. Er stellte unter anderem die KI-Perspektiven und die Förderaktivitäten der Cyberagentur vor. Der Einfluss von KI auf die Cyber-Bedrohungslandschaft wurde von Christoph Martin vom Bundesamt für Sicherheit in der Informationstechnik (BSI) thematisiert. Er warnte insbesondere vor der zunehmenden Reife von Social-Engineering-Angriffen in Text-, Ton-, Bild- und Videoform, die durch den Einsatz von KI immer ausgefeilter würden. Auch Malware werde inzwischen mit Hilfe von KI so optimiert, dass sie nicht mehr erkannt werden könne. Die Frage „Künstliche Intelligenz und Cyberspace – Wer profitiert mehr: Verteidiger oder Angreifer?“ stellte Andrea Martin von der IBM Deutschland GmbH. Noch gebe es ein Kopf-an-Kopf-Rennen zwischen beiden Seiten. Martin zeigte auf, wie KI-Lösungen den Menschen bei Sicherheitsaufgaben unterstützen

können. Dabei sei der Schutz von KI-Modellen und Trainingsdaten essentiell. Immer öfter sei zu beobachten, dass Unternehmen in Fragen der Cybersicherheit mit Partnern zusammenarbeiten und so ihr Schadensrisiko minimieren.

3 Fachausstellung und Workshops

Begleitet wurde die CODE-Jahrestagung von einer zweitägigen Fachausstellung. An beiden Veranstaltungstagen präsentierten sich ausgewählte IT-Unternehmen dem Fachpublikum und informierten über neueste Entwicklungen. In den Programmpausen hatten die Tagungsgäste zudem die Möglichkeit, in der „Coffee Corner“ Industrievorträge zu aktuellen Themen der Cybersicherheit zu hören.

Der weitere Nachmittag des ersten Veranstaltungstages stand ganz im Zeichen der Workshops. In insgesamt fünf parallel stattfindenden Workshops erwartete die Teilnehmer*innen ein breites Themenspektrum. Das Angebot reichte von Quantentechnologien über *Serious Games* bis hin zu Möglichkeiten, die Cybersicherheitsforschung zu lenken. Darüber hinaus traf sich die KI-Community der Bundeswehr in einem Workshop zum organisationsübergreifenden Informationsaustausch.

Zum Abschluss des ersten Veranstaltungstages beleuchtete Susanne Dehmel, Mitglied der Geschäftsleitung des Digitalverbands BITKOM e. V., in ihrem Vortrag das Thema Cybersicherheit aus Sicht der Wirtschaft. Ihr Plädoyer für eine stärkere Vernetzung der Akteure in diesem Bereich stieß beim Publikum auf große Zustimmung, ist dies doch einer der Grundgedanken der CODE-Jahrestagung. Beim Get-together, mit dem die Veranstalter*innen den ersten Tag ausklingen ließen, konnte dies dann auch gleich in die Tat umgesetzt werden.

4 Politische Keynotes und Innovationstagung

Den zweiten Tag auf der CODE-Jahrestagung eröffnete der Leitende Direktor Professor Wolfgang Hommel. Er begrüßte insbesondere die hochrangigen Gäste aus Politik und Bundeswehr und gab einen Überblick über die aktuellen Entwicklungen am Forschungsinstitut CODE. Mit über 50 laufenden Forschungsprojekten wurde ein neuer Höchststand erreicht. Die Drittmittel belaufen sich auf fast 30 Mio. €. Zudem konnten mit Marta Gomez-Barrero und Daniel Slamanig zwei neue Professuren besetzt werden. Neben Highlights aus den drei CODE-Geschäftsbereichen Cyber Defence, Smart Data und Quantum Technology, stellte der Leitende Direktor auch die Trainings- und Ausbildungsmöglichkeiten in der CODE-eigenen Cyber Range vor, die vor allem von Angehörigen der Bundeswehr, aber auch von Behörden genutzt werden. Ihm folgte Generalleutnant Michael Vetter. Der Abteilungsleiter CIT und CIO im Bundesministerium der Verteidigung sprach in seiner Keynote über „Software-defined Defence als neues Paradigma für die Fähigkeitsentwicklung der Streitkräfte“. Die sicherheitspolitische Zeitenwende gehe zeitgleich mit einer technologischen Zeitenwende einher. Verteidigung werde zunehmend von Software bestimmt – sie werde „*software-defined*“. Dabei spiele auch das Thema KI eine Rolle. Der Bundestagsabgeordnete Reinhard Brandl stellte in seinem Vortrag ein Zehn-

Punkte-Programm vor, mit dem die Zeitenwende auch in der Cyberabwehr umgesetzt werden kann. Die teilweise scharfen Kompetenzabgrenzungen zwischen Bund und Ländern würden der Bedrohungslage im Cyberraum nicht gerecht. Er warnte in diesem Zusammenhang davor, dass Angreifer diese Zuständigkeitsgrenzen gezielt ausnutzen könnten. Um als Staat insgesamt effektiver gegen Cyber-Bedrohungen vorgehen zu können, müssten Grenzen überwunden und Kooperationen gefördert werden – nicht nur zwischen Bund und Ländern, sondern auch zwischen öffentlicher Hand und Wirtschaft. Im Anschluss sprach der bayerische Staatsminister für Digitales, Fabian Mehring, zu den Tagungsteilnehmer*innen über Cybersicherheit und die Herausforderungen in diesem Bereich. Man dürfe nicht die Fehler der Vergangenheit wiederholen und sich im Zuge der Digitalisierung in neue Abhängigkeiten begeben und damit erpressbar machen, mahnte er. Dazu sei es besonders wichtig, die Hoheit über die eigenen Daten zu schützen, aber auch das Thema Cybersicherheit stärker in den Alltag der Menschen zu integrieren.

Den politischen Keynotes am Vormittag folgte die Innovationstagung Cyber/IT. Mit diesem Ideenwettbewerb will die Bundeswehr neue Wege gehen, um IT-Innovationen zu identifizieren und für eine mögliche Nutzung im Geschäftsbereich des BMVg zu gewinnen. Insgesamt gingen in diesem Jahr mehr als 30 Bewerbungen ein, aus denen eine fachkundige Jury bereits im Vorfeld die acht besten Konzepte auswählte und zur Teilnahme an der Konferenz einlud. Die acht Finalisten präsentierten dem Fachpublikum ihre Ideen in jeweils siebenminütigen Kurzvorträgen. Das Spektrum reichte von hochsicheren Routing-Architekturen in QKD-Netzen über neue Sensormodule für die halbautonome Gefechtsfeldaufklärung bis hin zu tragbaren Quantencomputern. Beim anschließenden „Meet-the-Speakers“ hatten die Gäste die Möglichkeit, mit den Vortragenden in Kontakt zu treten. Am Ende ging Simon Klenk von der SE3 Labs GmbH als Sieger hervor. Seine Idee einer Echtzeit-3D-Aufklärung durch autonome UAVs mit KI-Cockpit überzeugte die Fachjury und sicherte ihm ein Preisgeld von 15.000 €. Die Plätze 2 und 3 gingen an João Schneider von der Universität Gießen („Das VERITAS-System Hornisse: Lückenlose Lagebildung dank KI-gestützter Sensordatenauswertung“) und Markus Adrian Peter Beckers von der ARQUE Systems GmbH („Neuartige Chiparchitektur für einen kurzfristig verfügbaren transportablen Quantencomputer zum Einsatz direkt in Konfliktfällen für diverse Anwendungen“). Auch die weiteren Finalisten erhielten ein Preisgeld von 1000 €.

5 Science Track und Paneldiskussion

Das Nachmittagsprogramm begann nach einer Pause mit dem Science Track. Zwei Wissenschaftlerinnen und ein Wissenschaftler gaben dem Auditorium Einblicke in ihre aktuelle Forschung. Sabine Wölk vom Deutschen Zentrum für Luft- und Raumfahrt (DLR) sprach über Risiken und Potenziale des Quantencomputings. Professor Daniel Slamanig und Professorin Marta Gomez-Barrero, beide seit Ende 2023 am Forschungsinstitut CODE, stellten ihre Forschung zu „Kryptographie und KI“ bzw. „Biometrische Erkennung“ vor.

Der Nachmittag wurde mit den Vorträgen „Technologische Bedrohungen aus der Luft – Drohnen, Schwärme und Smart Dust als Risiken für kritische Infrastrukturen“ von Miriam Schnürer, Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI), und „Cyber & KI im Russlandkrieg“ von Volker Kozok, Netzwerk für Cyber Intelligence e. V., fortgesetzt.

In der abschließenden Podiumsdiskussion zum Thema „Innovation im Korsett – KI-Sicherheit in Deutschland“ kamen Expertinnen und Experten aus Militär und Industrie zu Wort. Mit dabei waren Kai Martius, Mitglied des Vorstands und Chief Technology Officer der secunet Security Networks AG, Miriam Schnürer, Mitglied des Vorstands beim Bundesverband für den Schutz Kritischer Infrastrukturen e. V., Cora Lisa Perner, R&T Cybersecurity, Airbus Defence and Space, Victoria Toriser, Cybergrundlagen und Innovation, Österreichisches Bundesheer, und Pascal van Overloop, Industry Advisor Defense & Intelligence bei der Microsoft Deutschland GmbH. Die Diskussion wurde von Felix Broßmann von der SKAD AG moderiert. Die Diskussion begann mit der Frage nach den Risiken, die mit dem Einsatz von KI-Technologien einhergehen. Derzeit birgt KI sowohl Chancen als auch Risiken. Die Einstufung von KI-Systemen als sicher und vertrauenswürdig scheiterte derzeit noch an der fehlenden Erklärbarkeit und einem tieferen Systemverständnis, so Martius. Eine Zertifizierung von KI-Systemen könne jedoch das Vertrauen der Menschen in ebendiese Systeme stärken. Zwar sehe der EU AI Act insbesondere für militärische Anwendungsbereiche (Defence, Military, National Security) weitreichende Ausnahmen vor, jedoch seien – abgesehen von wenigen Eigenentwicklungen für Spezialanwendungen – fast alle am Markt verfügbaren KI-Lösungen im Cyberbereich Dual Use. Damit unterliege man letztlich auch als militärischer Anwender dem KI-Gesetz, gab Toriser vom Bundesheer zu bedenken. Mit Blick auf die Sicherheitsproblematik von KI-Systemen wurden auch die Potenziale von Open-Source- und *On-Premise*-Ansätzen diskutiert. Zum Abschluss des Panels konnten die Diskutant*innen ihre Wünsche an eine zukünftige KI-Regulierung äußern. Hier wurde vor allem mehr Agilität auch bei der Zertifizierung und Standardisierung gefordert, die den technischen Fortschritt nicht ausbremst und sich stärker an den technischen Innovationszyklen orientiert – eben ein „regulatorisches Korsett, das stützt, aber noch ermöglicht zu atmen“, wie es Perner zusammenfasste. Auch die Forschung müsse noch an Themen wie der Erklärbarkeit von KI oder der Bias-Problematik arbeiten.

Mit dem Schlusswort von CODE-Direktor Professor Wolfgang Hommel endete das Vortragsprogramm der CODE-Jahrestagung 2024, die mit 540 Teilnehmenden die bisher größte CODE-Jahrestagung war. Er bedankte sich bei allen Teilnehmer*innen sowie bei allen Unterstützer*innen für ihr großes Engagement und lud zur nächsten Jahrestagung ein, die am 8. und 9. Juli 2025 stattfinden wird.

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und

die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen. Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

Hinweis des Verlags Der Verlag bleibt in Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutsadressen neutral.