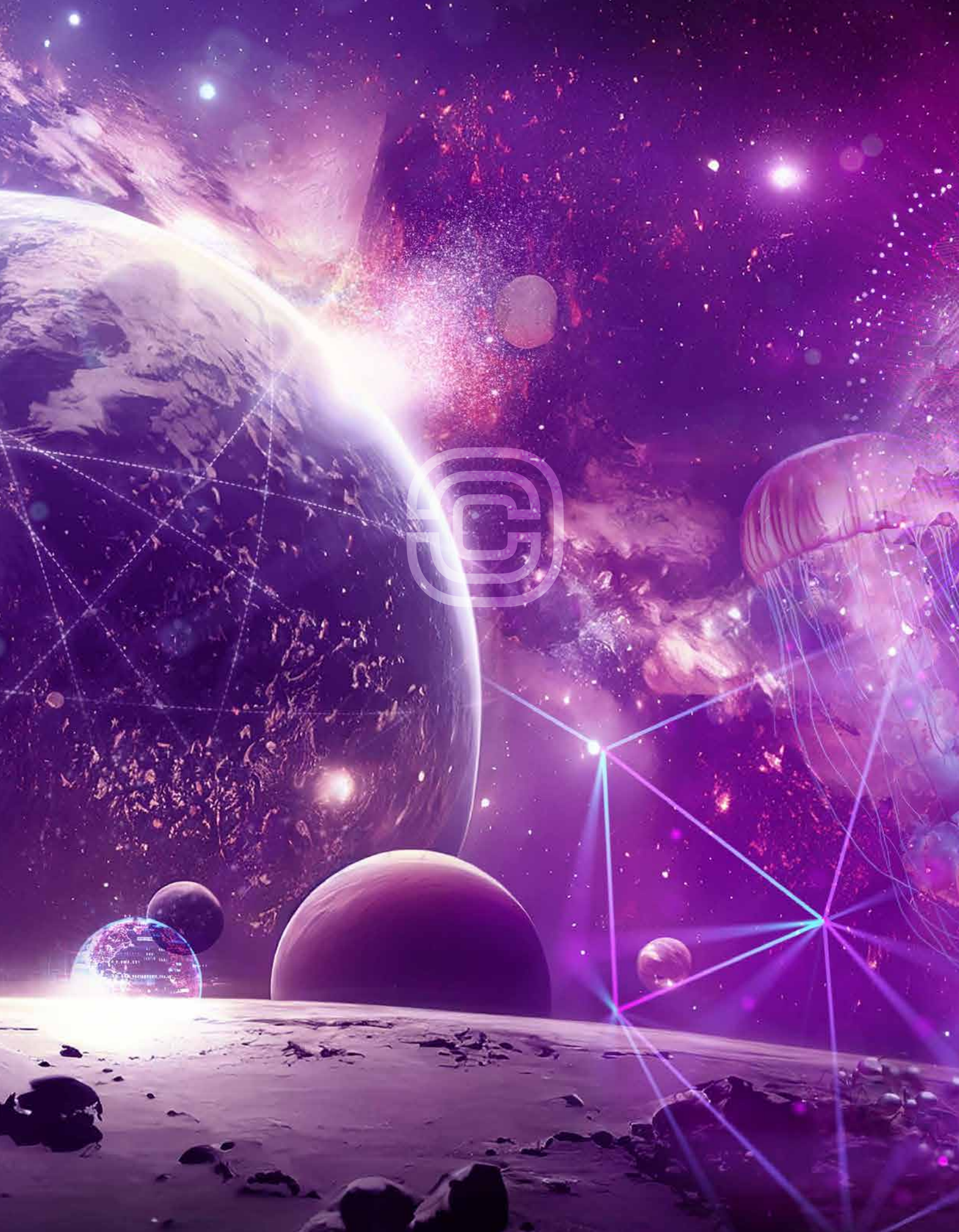
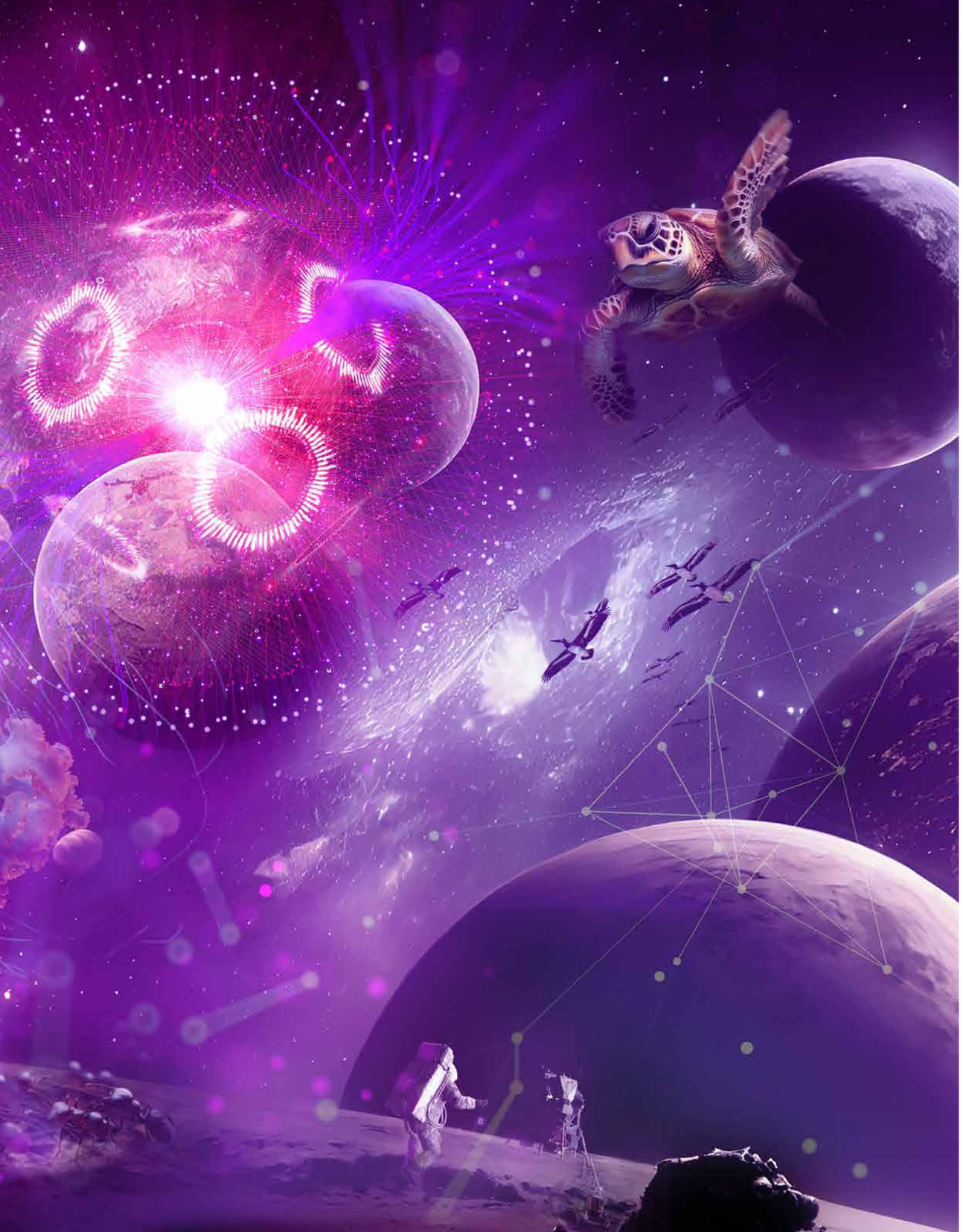




JAHRES FORSCHUNGS BERICHT

2024

cyberagentur

Zu Risiken und Nebenwirkungen:

Innovationskraft und Herausforderungen in der Cybersicherheitsforschung

Liebe Leserinnen und Leser,

die Agentur für Innovation in der Cybersicherheit – kurz Cyberagentur hat im kommenden Jahr 2025 ihren fünften Geburtstag. Als wir, Christian Hummert und Daniel Mayer, 2021 die Leitung der Cyberagentur übernahmen, hätten wir uns sicher nicht träumen lassen, wo wir jetzt nach drei Jahren stehen.

Fast 100 Mitarbeiterinnen und Mitarbeiter, viele fantastische Forschungsprojekte, die durch die Agentur initiiert wurden, und ein Ort der Innovation und disruptiven Ideen für die Cybersicherheit Deutschlands. Als Vision der Cyberagentur haben wir die beiden folgenden Sätze festgelegt:

„Wir stärken die Sicherheit und technologische Souveränität der Bundesrepublik Deutschland, durch Weiterentwicklung der Forschungslandschaft und von uns initiierte Forschungsprojekte. Wir haben den Anspruch, in der Cybersicherheit und damit verbundener Schlüsseltechnologien Teil der Weltspitze zu sein.“

Weltspitze – das ist kein kleiner Anspruch.

Während die DARPA nahezu jeder kennt, ist die kleine Schwester Cyberagentur vielen Menschen noch unbekannt. Trotzdem hat die junge Agentur mit coolen Forschungsprojekten wie Projekten zu Computer-Gehirn-Schnittstellen oder zum Mobilen Quantencomputer für Aufmerksamkeit gesorgt. Diese Projekte sind mehr als nur technologische Innovationen; sie sind Ausdruck unseres Engagements für eine sichere Zukunft und die Stärkung der digitalen Souveränität Deutschlands.

Der Fokus unserer Arbeit liegt in der Initiierung und Finanzierung von disruptiven Innovationen im Bereich der Cybersicherheit mit einem Blick auf die kommenden zehn bis 15 Jahre. Unsere Strategie umfasst die Schwerpunkte Sichere Gesellschaft, Sichere Systeme und Schlüsseltechnologien. Dabei steht die Agentur nicht alleine da, sondern arbeitet mit verschiedenen Partnern und Institutionen eng zusammen, um innovative Lösungen zu entwickeln und zu implementieren. Wir arbeiten eng mit der Bundesregierung, internationalen Organisationen und führenden Technologieunternehmen zusammen, um die Cybersicherheit auf nationaler und internationaler Ebene zu stärken. Dies prägt alle unsere Projekte. Wir legen besonderen Wert darauf, dass unsere Forschungsfragen nicht nur technologisch wegweisend sind, sondern auch den Anforderungen der Bedarfsträger in den Bundesministerien und ihren nachgeordneten Einrichtungen entsprechen. Dies ist ein wesentlicher Bestandteil unserer Arbeit, der sich in allen Projekten widerspiegelt.

Unsere Agentur ist kein klassisches Unternehmen und keine Behörde. Wir sind ein privatwirtschaftliches Unternehmen, dessen alleinige Gesellschafterin die Bundesrepublik Deutschland ist, vertreten durch das Bundesministerium der Verteidigung und das Bundesministerium des Innern und für Heimat.

In dieser besonderen Rolle, zwischen den Stühlen,

fühlen wir uns wohl und suchen unseren eigenen Weg. Furore machen nicht nur unsere Forschungsprojekte, sondern auch die innovativen Instrumente, diese zu beauftragen. Die Nutzung von Pre-Commercial-Procurement (PCP) zur Beauftragung von Forschung findet inzwischen mehr als nur Bewunderer. Es gibt auch Nachahmer in der öffentlichen Verwaltung. Und Forschung in einem Ideenwettbewerb zu vergeben, ist etwas, auf das wir sehr stolz sind.

Wir möchten diesen Rückblick nicht mit Eigenlob füllen, auch wenn wir glauben, zurecht Stolz auf das Erreichte sein zu können. Vielmehr sprechen wir Ihnen, liebe Leserinnen und Leser, unsere tiefe Dankbarkeit aus. Ohne die Unterstützung und das Vertrauen in unsere Arbeit wäre dies alles nicht möglich gewesen. Lassen Sie uns gemeinsam die Erfolge feiern und weiterhin mit Begeisterung und Engagement an der Cybersicherheit der Zukunft arbeiten.

Mit besten Grüßen,
Christian Hummert und Daniel Mayer

INTERVIEWS UND BERICHTE

CYBERAGENTUR EVALUIERT MIT HOHER EXPERTISE

Wettbewerb fördert innovative Forschungsansätze

Mit dem Wettbewerb:
„Existenzbedrohende Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien“ (HSK)
hat die Cyberagentur am Ende des letzten Jahres ein wichtiges Forschungsprojekt auf den Weg gebracht.

Ein Millionen-Auftrag zur Cybersicherheit Kritischer Infrastrukturen, der im September mit drei Forschungsverbünden in die zweite Phase startete.

Für die Bewertung der eingereichten Konzepte in der ersten Phase des Wettbewerbs hat die Cyberagentur eine Fachjury gebildet. Sie setzt sich für dieses Projekt aus Forscherinnen und Forschern der Cyberagentur und zwei externen Experten zusammen. Die externen Mitglieder sind Dr. Harald Niggemann, Cyber Security Strategist beim Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie Oberstleutnant Christoph Kühn, Dezernatsleiter im Zentrum für Cyber-Sicherheit der Bundeswehr. In einem Interview mit der Cyberagentur sprachen beide über den Wettbewerb, die inhaltlichen Herausforderungen und die Aussichten.

Frage: Wie wurden Sie für die Jury-Tätigkeit ausgewählt und wie ist Ihr Eindruck nach einem Jahr Jury-Tätigkeit?

Dr. Harald Niggemann: Der HSK-Wettbewerb* befasst sich mit einem Spektrum an Themen aus allen vier Säulen der Cybersicherheit: Prävention, Detektion, Attribution und Reaktion. Für das BSI stand daher von Anfang an fest, dass für diese Jury-Tätigkeit ein breiter Erfahrungshintergrund in unterschiedlichen Facetten notwendig ist.

Da ich seit vielen Jahren an strategischen Aspekten und Grundlagen der operativen Cybersicherheit im BSI arbeite und zudem bereits in anderen Projekten Jury-Erfahrungen sammeln konnte, habe ich diese Aufgabe natürlich sehr gerne übernommen. Das erste Jury-Jahr war für mich eine hervorragende Gelegenheit, mich intensiv mit neuen Forschungsansätzen zu befassen, und zwar nicht nur anhand der eingereichten Konzepte, sondern auch im Austausch mit den anderen Jury-Mitgliedern.

Christoph Kühn: Im Juli 2022 wurden mögliche Jury-Mitwirkende für dieses Projekt gesucht. Da mich Wissenschaft und Forschung interessieren und das Projekt meiner aktuellen Aufgabe ähnlich ist, habe ich mich beworben. Mein Dezernat im Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw) befasst sich mit Cyber-Bedrohungen, -Gefährdungen und -Risiken. Das ZCSBw als Ganzes schützt die Informationen und die Informationstechnik der Bundeswehr in verschiedenen Aspekten. Meine Vorgesetzten unterstützten das Engagement, auch wenn wir uns alle bewusst waren, dass hier zusätzliche Arbeit und Aufwand notwendig sind. Anscheinend passte alles und ich wurde ausgewählt.

Die Arbeit macht Spaß, obwohl viel Zeit investiert werden muss. Gerade in den Phasen, in denen Dokumente evaluiert werden müssen, komme ich nicht umhin, diese auch in der Freizeit zu lesen und zu kommentieren. Über mehrere Tage hinweg Stunden im Büro zu sitzen, um konzentriert zu lesen, ist als Dezernatsleiter in einem operativen Bereich einfach nicht drin. Das Team der Cyberagentur bindet uns zwei Externe sehr gut ein und man erkennt, dass auf unsere Meinung Wert gelegt wird. Deshalb wende ich die Zeit gerne auf.

Frage: Worin sehen Sie die Bedeutung des laufenden Wettbewerbs? Was erhoffen Sie sich von dem Wettbewerb?

Dr. Harald Niggemann: Cyberangriffe entwickeln sich sowohl technologisch als auch hinsichtlich der Vorgehensweisen ständig weiter. Sie betreffen alle Gesellschaftsbereiche, insbesondere auch die Kritischen Infrastrukturen, also Dienstleistungen, die für die Versorgung der Bevölkerung besonders wichtig sind. Ohne innovative Ansätze, die auf wissenschaftlichen Erkenntnissen basieren, werden wir diesen Gefahren zukünftig nicht adäquat entgegenwirken können. Dafür benötigen wir die gesamte Kette von der Grundlagenforschung bis hin zur Entwicklung marktfähiger Produkte. Der HSK-Wettbewerb ist hierzu ein wichtiger Beitrag, denn er ermöglicht die Beauftragung von herausragenden Forschungsvorhaben, die die ausgetretenen Pfade verlassen.

Christoph Kühn: Die Cyberagentur fördert mit dem Projekt hochrisikobehaftete Forschung. Ich glaube nicht, dass insbesondere bei Firmen und Startups, aber auch bei Universitäten, welche auf Drittmittel angewiesen sind, ohne die Projektmittel der Cyberagentur an diesen Themen so intensiv geforscht werden könnte. Genau hierfür ist die Cyberagentur gegründet worden: die Souveränität Deutschlands auch in der Cybersicherheit und ihren Schlüsseltechnologien sicherzustellen. 2024 hat der Bundesminister der Verteidigung die Entscheidung getroffen, den Organisationsbereich CIR zu einer Teilstreitkraft zu verändern. Während ein Organisationsbereich „nur“ unterstützend tätig ist, kann eine Teilstreitkraft militärische Handlungen in einem bestimmten Raum vornehmen und Verantwortung für diesen tragen. Dies zeigt deutlich, dass der Cyber- und Informationsraum (CIR) eine militärische Domäne ist, die umkämpft wird und verteidigt werden muss.

Auch die NATO hat in den letzten Monaten deutliche Aussagen getroffen und Schritte eingeleitet, um den Cyberspace noch umfassender ständig, auch ohne die Ausrufung von Artikel 4 oder 5 des NATO-Vertrages, zu überwachen und zu verteidigen. Sowohl national als auch international wurde also erkannt und Rechnung getragen, dass KRITIS ein Ziel für Gegner im Cyberspace darstellen. Und diesen kann man nicht mit mechanischen Waffen, sondern nur durch moderne Technik, durchdachte Prozesse und kluge Köpfe verteidigen. Alles drei wird im Wettbewerb gefördert. Wir werden die Forschungsergebnisse nicht unmittelbar einsetzen können. Aber wenn wir auf die Laufzeit von Rüstungsprojekten schauen, wird klar, dass wir weit in die Zukunft blicken müssen, um diese bereits im Design sicher zu gestalten. Auch wenn die Bundeswehr gemäß Definition nicht zur Kritischen Infrastruktur zählt, ist die Einsatzfähigkeit der Bundeswehr essenziell für Deutschland.

Frage: Was sind Problemfragen, die an die künftige Cybersicherheit der Kritischen Infrastrukturen gestellt werden?

Christoph Kühn: Unsere Welt ist geprägt von Komplexität und Vernetzung. Dies führt unweigerlich dazu, dass Systeme Angriffsflächen bieten, welche mit heutigen Mitteln und verfügbarem Fachpersonal nicht immer ausreichend geschützt werden können. Deshalb benötigen wir Verfahren und Werkzeuge, die uns dabei unterstützen, Angriffe im Cyber- und Informationsraum zu verhindern, zu detektieren und darauf zu reagieren. Natürlich spielt hier auch immer das Thema künstliche Intelligenz eine wichtige Rolle. Schließlich müssen wir davon ausgehen, dass auch Angreifer diese Methoden nutzen. Sehr gut gefällt mir, dass alle verbliebenen Konsortien nicht nur Einzelaspekte betrachten, sondern einen holistischen Ansatz gewählt haben.

Dr. Harald Niggemann: Ich möchte zwei Aspekte herausgreifen, die aus meiner Sicht besonders wichtig sind. Der Erste ist die Notwendigkeit zur Automatisierung. Cyberangriffe betreffen oft viele Systeme gleichzeitig und erfordern häufig sehr schnelle Aktivitäten, um den potenziellen Schaden zu begrenzen. Manuelles Eingreifen wird hierfür immer weniger praktikabel. Der zweite Aspekt ist die Sicherheit in der gesamten Lieferkette. In den vergangenen Jahren stand vor allem der sichere Betrieb bei den Anwendern von Informationstechnik im Vordergrund. Wir werden aber nur dann eine angemessene Cybersicherheit gewährleisten können, wenn wir dies von Anfang an bei der Entwicklung von Komponenten und Zulieferkomponenten mitdenken.

Fortsetzung >

** Erklärung HSK: Existenzbedrohende Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien*

Fortsetzung Interview

Frage:

**Sie sind beide in einer eher operativen Rolle tätig.
Welchen Eindruck haben Sie von der akademischen Seite gewonnen und gibt es Erkenntnisse (fachlicher oder prozessualer Natur), die Sie für Ihre Tätigkeit übernehmen können?**

Dr. Harald Niggemann: Die Arbeitsweise und die Dienstleistungen des BSI, auch im Bereich der operativen Cybersicherheit, basieren auf wissenschaftlichen Erkenntnissen. Der kontinuierliche Austausch mit universitären und außeruniversitären Forschungseinrichtungen ist daher eine wesentliche Grundlage unserer Arbeit. Der besondere Mehrwert des HSK-Wettbewerbs liegt aus meiner Sicht im Wagnis. Die Cyberagentur erwartet in diesem Wettbewerb von den Antragstellern die Bereitschaft, abseits der bekannten Ansätze nach neuen Lösungen zu suchen, auch wenn dadurch der Verlauf des Vorhabens weniger gut vorhersagbar wird. Bereits jetzt konnte ich aus den bewerteten Konzepten zahlreiche Ideen lernen und die Hauptergebnisse liegen ja erst noch vor uns.

Christoph Kühn: Ich wurde wunderbar aufgenommen und meine Meinung wird geschätzt, obwohl ich der Einzige ohne Doktortitel in der Jury bin (lacht). Gerade der Mix aus akademischem und operativem Personal in der Jury macht es möglich, Projekte differenziert zu bewerten. Auch wenn ich im operativen Bereich tätig bin, so bringt meine Position als Dezernatsleiter mit sich, dass ich häufig Dokumente und Inhalte erfassen, Schwerpunkte und Schlüsselaussagen erkennen, diese bewerten und Schlussfolgerungen ziehen muss. Dies ist von akademischer Arbeit nicht weit entfernt.

Es war für mich interessant, die unterschiedlichen Ansätze der Wettbewerber sowie deren Sicht auf das Gesamtproblem zu sehen. Diese haben mir neue Zusammenhänge erschlossen, die ich wahrscheinlich sonst nicht gesehen hätte. Davon habe ich schon in anderen Arbeitsgruppen, aber auch in meiner täglichen Arbeit, profitieren können. Häufig entwickeln Gruppen über die Jahre eine eigene Fachsprache. Für die Bundeswehr und ihre Abkürzungen ist dies ja sogar sprichwörtlich. Auch hier musste ich mich erstmal wieder daran gewöhnen, Fachbegriffe der anderen zu verstehen und mich selbst mit meinen zurückzuhalten. Auch dies ist ein Softskill, den ich verbessern konnte.

Wie profitieren Ihre Organisationen von Ihrer Tätigkeit als Jury-Mitglied?

Dr. Harald Niggemann: Zum einen ist die Jury-Mitgliedschaft eine weitere Möglichkeit für das BSI, seine Erfahrungen in der Prävention, Detektion und schadensmindernden Reaktion in die Forschungslandschaft einzubringen. Dies gilt beispielsweise für die praktische Arbeit im Nationalen IT-Lagezentrum und im Computer Emergency Response Team Bund (CERT-Bund), die beide im BSI angesiedelt sind. Genauso wichtig ist dem BSI aber auch der umgekehrte Informationsfluss. Wie bereits dargestellt, ist die Cybersicherheit auf neue Impulse aus Forschung und Wissenschaft angewiesen.

Christoph Kühn: Mit mir als Teil des externen Juryteams werden vorhandene Expertisen um den Blickwinkel militärische Verteidigung erweitert und die sich bewerbenden Projektgruppen aufgefordert, sich hierzu ebenfalls Gedanken zu machen. Für mich hat sich insbesondere gezeigt, dass die unmittelbaren Gespräche bei Workshops vor Ort oder in längeren Web-Konferenzen die Zusammenarbeit und das gegenseitige Verständnis verbessern.

*Foto: Dr. Harald Niggemann,
Cyber Security Strategist beim Bundesamt für Sicherheit in der Informationstechnik (BSI)*

Im fachlichen Dialog oder auch bei Nebengesprächen kommt man plötzlich auf Dinge, welche in einer schriftlichen Kommentierung oder E-Mail nicht thematisiert worden wären. Hierbei werden auch Themen angeschnitten, welche für andere Projekte relevant sind oder die allgemeine militärische Sicht verdeutlichen. Deshalb halte ich den Aufwand für Präsenz vor Ort für mehr als gerechtfertigt.

Welchen Rat würden Sie künftigen Jury-Mitgliedern mit auf den Weg geben?

Christoph Kühn: Freuen Sie sich auf die Arbeit und die Erfahrungen und treten Sie locker und gelassen in die akademische Welt ein. Dies ist aber keine Aufgabe, die mit einigen wenigen kurzen Besprechungen getan ist. Bis jetzt habe ich über 20 Arbeitstage investiert und das Projekt läuft noch über drei Jahre. Den Aufwand ist es sicherlich wert, aber man muss die Zeit im eigenen Terminplan und Aufgabenportfolio auch finden können.

Dr. Harald Niggemann: Als Jury-Mitglied habe ich mir zum Ziel gesetzt, bei der Bewertung der Einreichungen einerseits natürlich auf meine Erfahrungen auf dem Gebiet der Cybersicherheit zurückzugreifen, andererseits aber auch bereit zu sein, die etablierten Lösungen in Frage zu stellen. Um zu möglichst objektiven Bewertungen zu kommen, muss ich mich auf neue Ansätze einlassen können, sofern sie fundiert, plausibel und erfolgversprechend sind.

*Foto: Oberstleutnant Christoph Kühn,
Dezernatsleiter im Zentrum für Cyber-Sicherheit der Bundeswehr*

Projekt ATTRIBUT:

Verborgene Cyber-Bedrohungen entlarven und Täter zur Verantwortung ziehen

Seit September 2022 arbeite ich mit meinem Team an der Otto-von-Guericke-Universität Magdeburg an einem der spannendsten Forschungsprojekte unserer Zeit: dem Projekt ATTRIBUT. Dieses Projekt ist Teil des Wettbewerbs „Existenzbedrohende Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien“ (HSK), der von der Cyberagentur initiiert wurde. Unser Ziel ist es, neue Methoden zur Detektion und Attribution von Schadcode aufzuzeigen, der sich auf versteckte Kommunikationswege und steganographische Techniken, auch Information Hiding genannt, stützt.

Stego-Malware, die verdeckte Kommunikationskanäle nutzt, um Informationen unbemerkt zu exfiltrieren oder Command & Control-Kommunikation zu verbergen, stellt eine wachsende Bedrohung für die Cybersicherheit dar. Diese Schadsoftware bleibt oft unentdeckt und infiltriert selbst in gut gesicherte Systeme. Das Projekt ATTRIBUT zielt darauf ab, diese verdeckten Bedrohungen frühzeitig zu identifizieren und die digitalen Angriffe zuverlässig den Urhebern zuzuordnen.

Im ersten Jahr unseres Forschungsprojekts konnten wir bereits vielversprechende Ergebnisse erzielen. Wir haben gezeigt, dass es möglich ist, individuelle Merkmale in den Spuren von Schadcode zu erkennen und diese exakt zu beschreiben. Diese Merkmale sind oft gut verborgen und erfordern eine genaue Analyse, um eine verlässliche Attribution zu ermöglichen. Eine der größten Herausforderungen dabei ist die enorme Vielfalt an potenziellen Versteckmöglichkeiten, die es Angreifern erlaubt, ihre Spuren auf unterschiedlichste Weise zu verschleiern.

Unser Ansatz erfordert nicht nur die technische Fähigkeit zur Detektion, sondern auch die Verknüpfung der digitalen Spuren mit den realen Identitäten der Täter. Dies ist besonders komplex, da Angreifer ausgeklügelte Methoden nutzen, um ihre wahre Identität zu verschleiern. Unser Ziel ist es, diese Verbindungen trotz Fehlern, Verlusten und Unsicherheiten belastbar zu erkennen und zu dokumentieren.

Das Projekt ATTRIBUT bietet das Potenzial, sicherheitskritische Infrastrukturen besser zu schützen und die digitalen Angreifer rechtlich zur Verantwortung zu ziehen. Die Arbeit, die wir leisten, könnte die Forschung im Bereich inneren und äußeren Souveränität nachhaltig beeinflussen und unsere digitale Welt sicherer machen.

Kurzvita

Prof. Dr.-Ing. Jana Dittmann ist seit 2002 Professorin für Mediensicherheit an der Otto-von-Guericke-Universität Magdeburg und leitet die Arbeitsgruppe „Multimedia and Security“ (AMSL). Ihre Forschungsschwerpunkte umfassen Information Hiding, digitale Wasserzeichen, Benutzerauthentifizierung und Forensik. Mit umfangreicher Erfahrung aus nationalen und internationalen Projekten zählt sie zu den führenden Expertinnen auf ihrem Gebiet.

Foto: Prof. Dr.-Ing. Jana Dittmann - Projektleiterin und Professorin an der Otto-von-Guericke-Universität Magdeburg

Projekt SOVEREIGN:

KI-basierte Resilienz für die Cybersicherheit Kritischer Infrastrukturen

Angesichts der zunehmenden Bedrohungen im digitalen Raum hat sich meine Forschungsgruppe an der Universität Hamburg der Aufgabe verschrieben, innovative Methoden zur Erkennung und Abwehr von Cyberangriffen zu entwickeln. Das Projekt SOVEREIGN, das im Rahmen des HSK-Wettbewerbs der Cyberagentur ins Leben gerufen wurde, stellt einen bedeutenden Schritt in diese Richtung dar. SOVEREIGN verfolgt einen ganzheitlichen Ansatz zur Erhöhung der Cybersicherheit und Souveränität Kritischer Infrastrukturen durch die Entwicklung einer modularen Cyber-Defense-Plattform auf Basis von KI und Zero-Trust.

In einer Zeit, in der Cyberangriffe immer raffinierter werden, gilt es Vertrauensbeziehungen zu minimieren und auch diese wenigen Beziehungen kontinuierlich in Frage zu stellen (Zero-Trust). Unsere Plattform verfolgt daher einen konsequenten Ansatz, bei dem jede Interaktion im Netzwerk kontinuierlich validiert wird und Komponenten und deren Interaktion kontinuierlich beobachtet werden. Dies ermöglicht es, potenzielle Bedrohungen sofort zu identifizieren und geeignete Gegenmaßnahmen einzuleiten.

Die modulare Architektur von SOVEREIGN integriert dazu passive und aktive Sensoren tief in die Kritischen Infrastrukturen. Diese Sensoren erkennen verdächtige Aktivitäten frühzeitig und leiten automatisierte Reaktionen ein. Durch den Einsatz von Künstlicher Intelligenz (KI) kann die Plattform Angriffe nicht nur erkennen, sondern auch Risiken bewerten und dynamische Abwehrstrategien entwickeln, bevor Schäden auftreten.

Ein wesentlicher Aspekt des Projekts ist der Zugang zu realen Daten aus Kritischen Infrastrukturen. Diese Daten sind entscheidend für die realitätsnahe Evaluation und kontinuierliche Verbesserung unserer Lösungen. Hierfür haben wir uns mit führenden Industriepartnern zusammengeschlossen, die uns ihre Expertise und Ressourcen zur Verfügung stellen. Die Zusammenstellung dieses Konsortiums war eine herausfordernde, aber notwendige Aufgabe, um die komplexen Anforderungen des Projekts zu erfüllen.

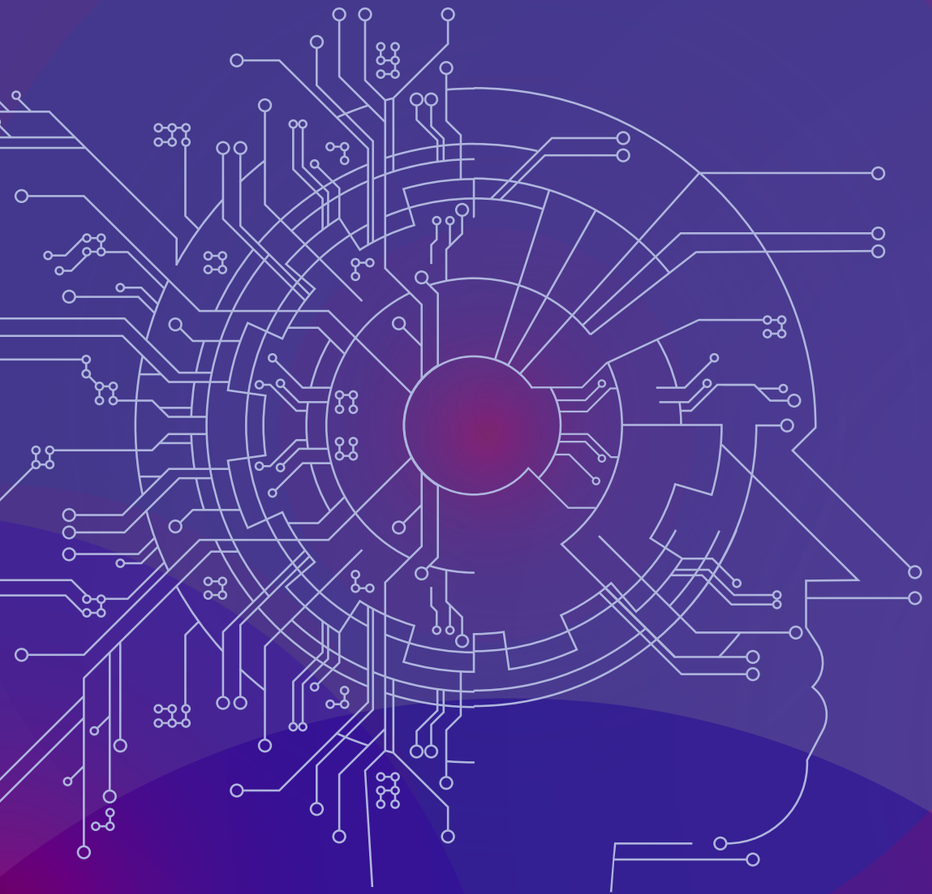
Besonders spannend für uns war die Teilnahme am Pre-Commercial Procurement (PCP)-Verfahren der Cyberagentur. Dieser Wettbewerb bot uns die Gelegenheit, unsere besten Ideen in einem hochkompetitiven Umfeld zu präsentieren und weiterzuentwickeln. Dass wir es in die dritte Phase des Wettbewerbs geschafft haben, unterstreicht die Qualität und das Innovationspotenzial unserer Arbeit.

In den nächsten drei Jahren werden wir intensiv daran arbeiten, die entwickelten Konzepte umzusetzen und SOVEREIGN zu einer Plattform zu machen, die die Cybersicherheit in Kritischen Infrastrukturen auf ein neues Niveau hebt. Wir sind überzeugt, dass die Ergebnisse dieses Projekts einen erheblichen Beitrag zum Schutz unserer digitalen Welt leisten werden.

Kurzvita

Prof. Dr. Mathias Fischer ist Professor für Netzwerk- und IT-Sicherheit an der Universität Hamburg. Er forscht seit vielen Jahren an skalierbaren und präzisen Methoden zur Erkennung von Cyber-Angriffen und ist ein führender Experte auf diesem Gebiet. Mit seiner umfassenden Erfahrung in der Zusammenarbeit mit nationalen und internationalen Partnern leitet er das Projekt SOVEREIGN, das sich auf die Entwicklung einer zukunftsweisenden Cyber-Defense-Plattform konzentriert. Seine Arbeit trägt maßgeblich zur Stärkung der Cybersicherheit bei.

Foto: Prof. Dr. Mathias Fischer- Projektleiter und Professor für Netzwerk- und IT-Sicherheit an der Universität Hamburg



Das Cottbuser Startup Zander Laboratories GmbH hat einen bedeutenden Schritt in der Entwicklung der Mensch-Maschine-Interaktion gemacht. Mit einem Auftragsvolumen von 30 Millionen Euro, das am 15. Dezember 2023 von der Cyberagentur vergeben wurde, plant das Unternehmen innerhalb von vier Jahren neurotechnologische Prototypen zu entwickeln.

Diese sollen die Interaktion zwischen Mensch und Maschine sowie künstlicher Intelligenz revolutionieren. Hochriskante Eingriffe ins Gehirn zur Steuerung von Maschinen sollen damit überflüssig werden.

Das NAFAS Projekt

Prof. Dr. Thorsten Zander, Geschäftsführer von Zander Laboratories und Lichtenberg-Professor für Neuroadaptive Mensch-Technik-Interaktion an der Brandenburgischen Technischen Universität Cottbus-Senftenberg, hat das Projekt „Neuroadaptivität für autonome Systeme“ (NAFAS) mit seinem Team voller Freude und Tatendrang gestartet. „Es ist unser erklärtes Ziel, die Interaktion zwischen Mensch und Technologie neu zu gestalten: Wir streben nach Systemen, die sich intuitiv dem individuellen Nutzer anhand dessen Hirnaktivität anpassen können und nach KI-Anwendungen, die unmittelbar vom menschlichen Gehirn lernen“, erklärt Zander.
„Wir haben die Ankündigung dazu auf den Seiten der Cyberagentur gesehen und uns sehr gefreut, dass die Ausschreibung ermöglichen wird, dieses wichtige Themenfeld weiterzubringen“, berichtet Zander. Die Ausschreibung bot eine vielversprechende Gelegenheit, das Gebiet der Brain-Computer Interfaces (BCIs) voranzutreiben.

30 Millionen für Mensch X Maschine Interaktion

Expertise und Forschungsansatz

Prof. Dr. Zander bringt eine umfangreiche Expertise in das Projekt ein: „Ich habe das Forschungsfeld der Passiven Brain-Computer Interfaces (BCIs) ab dem Jahr 2008 eingeleitet und seitdem intensiv untersucht. Dabei habe ich mit meiner Forschergruppe neue Methoden zur Erkennung von Hirnprozessen entwickelt und präzise Validierungsmethoden für diese Ansätze auf den Weg gebracht.“ Besondere Meilensteine beinhalten die Echtzeiterkennung mentaler Prozesse und der Nachweis, dass eine KI direkt vom menschlichen Gehirn lernen kann. Zusammen mit Prof. Stephen Fairclough aus Liverpool hat Zander zudem das Forschungsfeld der Neuroadaptiven Technologien etabliert.
Der Forschungsauftrag ermöglicht es, Technologien aus dem Labor näher in die Realität zu bringen. „Des Weiteren können Fragen beantwortet werden, die bisher aus Mangel an Forschungsgeldern nicht angegangen werden konnten, obwohl sie extrem wichtig und weitreichend sind“, betont Zander. Die Entwicklung neuroadaptiver Systeme wird somit beschleunigt und praxisnah umgesetzt.

Erwartungen an die Ergebnisse

„Die Ergebnisse des Projektes werden dazu beitragen, künstliche und menschliche Intelligenz näher zusammenzubringen“, so Zander. Dies würde die Kommunikation mit Maschinen revolutionieren, indem sie intuitiver und empathischer gestaltet wird. „Das resultierende bessere Verständnis, was die Maschinen für den Menschen entwickeln, wird dazu führen, dass KIs generell sicherer und hilfreicher werden.“

Die Umsetzung des Forschungsauftrags brachte bereits einige Herausforderungen mit sich. „Momentan war das größte Problem genügend Talente zu finden, die uns bei dem Projekt helfen können“, erklärt Zander. Trotz über 950 Bewerbungen war eine intensive Auswahl notwendig. Zudem mussten Kooperationen mit Partnern aus Wissenschaft und Industrie koordiniert werden. „Wir sind jedoch enorm zufrieden mit dem Fortschritt und freuen uns sehr auf die nächsten Schritte“, fasst Zander die bisherigen Erfahrungen zusammen.

Mit diesem Projekt der Cyberagentur steht Zander Laboratories an der Spitze der Forschung zur neuroadaptiven Mensch-Maschine-Interaktion und zeigt das immense Potenzial, das in der Verbindung von Gehirn und Technologie steckt.

Foto: Prof. Dr. Thorsten Zander, Geschäftsführer von Zander Laboratories und Lichtenberg Professor für Neuroadaptive Mensch-Technik-Interaktion an der Brandenburgischen Technischen Universität Cottbus-Senftenberg

Spannendes Duo im Forschungsumfeld zukünftiger Cyberkriminalität:

Interdisziplinarität und Dynamik

Als die Cyberagentur im Februar 2024 zur Teilnahme an zwei Wettbewerben zu Zukünftiger Cyberkriminalität aufrief, stand bereits fest, dass man sich auf einem weitgehend unerforschten Terrain bewegen werde. Schließlich geht es erstmals in einem interdisziplinären Projekt um zukünftige Entwicklungen im Hinblick auf das Zusammenspiel von technologischen, kulturellen und strukturellen Aspekten der Cyberkriminalität. Für die Begleitung und Bewertung der forschenden Einrichtungen suchte sich das Team aus Halle auch externe Jury-Mitglieder.

Mit Dr. Patrick Voss - de Haan fanden sie einen Fachmann, der auf eine lange Erfahrung im Bundeskriminalamt (BKA) bauen kann und der sich auf Cybercrimeforschung spezialisiert hat:

Das Kriminalistische Institut ist im BKA für die Cybercrimeforschung zuständig und pflegt enge Kontakte zur Cyberagentur, weil viele Aspekte der Cybercrimeforschung wichtige Elemente der Cybersicherheit insgesamt betreffen.

Die Erfahrung und Kompetenz, die im Kriminalistischen Institut des BKA über die letzten Jahre aufgebaut werden konnten, dürften ein wichtiger Aspekt für die Cyberagentur bei der Auswahl für die Jury gewesen sein. Umgekehrt sind die Möglichkeiten, die sich durch die Forschungsfinanzierung der Cyberagentur für die Cybercrimeforschung bieten, für das BKA wichtig, dass aktuelle Bedarfe der Polizei angemessen und effektiv behandelt werden können.

Seit über 20 Jahren bin ich beim BKA und seit über 15 Jahren beschäftige ich mich intensiv mit unterschiedlichsten Cyberthemen. Das hat mich nicht nur schon früh mit technologischen Entwicklungen beispielsweise Künstlicher Intelligenz, Kryptowährungen und Blockchain-Technologie in Kontakt gebracht, sondern auch mit vielen Formen der Cyberkriminalität. Auch diverse Erfahrungen mit IT- und Forschungsprojekten dürften hilfreich sein.
Eine besonders ungewöhnliche Kompetenz könnte aber durch die Brückenfunktion entstehen, die das Kriminalistische Institut einnimmt:

Es vermittelt zwischen den sehr unterschiedlichen Welten der Polizeifachlichkeit und der sozialwissenschaftlichen Forschung, wobei im Bereich der Cyberkriminalität noch die Welt der Technik hinzukommt. Ich bin gespannt, wie viel Flexibilität der gesamte Projektablauf durch den Wettbewerb und die iterative Ausarbeitung der Projektkonzepte gewinnt und wie sich dies auch in der Qualität der Ergebnisse niederschlägt.

Die direkte Konkurrenzsituation der Teilnehmenden kann anspornend und belebend wirken, aber mehr noch dürfte das wiederholte Feedback, das die Teilnehmer erhalten, eine noch höhere Qualität der Projektkonzepte möglich machen.

Im Forschungsauftrag sehe ich eine besondere Herausforderung darin, in einem sehr umfangreichen und interdisziplinären Themenbereich relevante Schwerpunkte zu setzen, sowohl in Bezug auf technologische und gesellschaftliche Entwicklungen als auch in Bezug auf Kriminalität.

Die Vielfalt der beteiligten Faktoren führt zu einer sehr hohen Komplexität der zu behandelnden Fragestellungen. Zur großen Dynamik der technologischen Entwicklungen kommt hinzu, dass es für Cyberkriminalität, als vergleichsweise neues Forschungsgebiet, wesentlich weniger wissenschaftliche Vorarbeiten gibt als für viele andere Kriminalitätsphänomene.

Ich hoffe, in der Jury dazu beizutragen, dass die Projektergebnisse bei hoher Qualität möglichst genau den polizeilichen Bedarf treffen. Wenn dies gelingt, dann können die Ergebnisse nicht nur für das BKA, sondern für die Polizei in Bund und Ländern insgesamt sehr wertvoll sein.

Das gilt sowohl für die Möglichkeit zur Reaktion auf kurz- und mittelfristige Entwicklungen, wenn sie sich durch Musteranalysen entdecken lassen, als auch für die Möglichkeit, sich strategisch auf langfristige Entwicklungen einzustellen, wenn sich dafür Hinweise aus Zukunftsanalysen ableiten lassen.

Foto: Dr. Patrick Voss - de Haan,
Fachmann im Bundeskriminalamt (BKA) und Spezialist der Cybercrimeforschung

Zukunftsprojekte ermöglichen:

Der Wissenschaftliche Dienst als Unterstützer und Impulsgeber

Der Wissenschaftliche Dienst analysiert und formt den strategischen, rechtlichen und bedarfsorientierten Bezugsrahmen für Forschungsvorhaben des Bereichs Forschung und Innovation (F&I) und unterstützt diesen in der Umsetzung und Organisation der Vorhaben.
Dabei fungiert der Wissenschaftliche Dienst auch als zentrale Schnittstelle zwischen Wissenschaft und Verwaltung. Er umfasst die Referate Innovations- und Wissensmanagement, Projektmanagement, Geistiges Eigentum und Verbindungswesen.

Die Arbeit des Innovations- und Wissensmanagements trägt dazu bei, die Cyberagentur als relevante Akteurin im nationalen und internationalen Innovationsökosystem zu positionieren. Durch qualitative und quantitative Trend- und Szenarioanalysen sowie den strategischen Austausch mit dem Ökosystem können schwache Signale erkannt und Projektimpulse generiert werden. Das Innovationsmanagement konnte bereits beachtenswerte Projekte wie die Cyberagentur Startup Landscapes Deutschland und Israel sowie die Business Landscape Quantum abschließen. In Arbeit und Planung befinden sich weitere geographische und thematische Landscapes. Der Bereich Data Science wird ebenfalls ausgebaut, um die quantitative Auswertung strukturierter Forschungsdaten voranzutreiben. Als Multiplikator stellt das Referat gewonnenes Wissen sowohl der Cyberagentur als auch den Bedarfsträgern zur Verfügung und sorgt für dessen nachhaltige Nutzung.

Das Projektmanagement unterstützt bei der Initialisierung, Durchführung und erfolgreichen Umsetzung der Projekte und übernimmt zudem die Organisation des Projektcontrollings. Auch interne Projekte werden begleitet, um die zielführende Planung, Durchführung und Evaluation sicherzustellen. Mit klassischen und agilen Methoden sowie einem hohen Maß an Sachverstand und Fingerspitzengefühl wird die Qualität der Prozesse garantiert, wobei die Zufriedenheit der Stakeholder im Vordergrund steht.

Ein weiterer zentraler Bereich ist die Sicherung und Verwaltung des in den Forschungsprojekten entstehenden geistigen Eigentums. Das zuständige Referat zielt auf eine umfassende IP-Sicherung für den Bund, die zugleich den Auf- und Ausbau der deutschen Foschungs- und Entwicklungslandschaft im Bereich Cybersicherheit ermöglicht.

Das Verbindungswesen der Cyberagentur identifiziert Bedarfe und Themen der Inneren und Äußeren Sicherheit und setzt dabei auch auf innovative Workshopformate. Das Referat knüpft und pflegt wichtige Kontakte und dient als zentraler Ansprechpartner (SPoC) für Partner im behördlichen Ökosystem. Auf diese Weise wird eine effektive Kommunikation zwischen den Bedarfsträgern der Inneren und Äußeren Sicherheit und dem Forschungsbereich der Cyberagentur gewährleistet, was die Initiierung konkreter Projekte vorantreibt.

Dieser umfassende Ansatz des Wissenschaftlichen Dienstes zeigt die vielfältigen Aktivitäten der Cyberagentur im Bereich der Forschungs- und Innovationsförderung sowie die strategische Verknüpfung mit sicherheitsrelevanten Bedarfsträgern.

Die Trendscouts:

Innovatives Wissen für eine sichere Zukunft

Das Innovations- und Wissensmanagement der Cyberagentur identifiziert potenziell bahnbrechende Innovationen im Bereich der Cybersicherheit und den dazugehörigen Schlüsseltechnologien. So leistet dieses Referat der Cyberagentur seinen Beitrag zur technologischen Souveränität Deutschlands im Cyber- und Informationsraum. Es ist folglich in der Cyberagentur für die Trend-, Szenario-, und Foresightanalysen zuständig. Durch qualitative und quantitative Trend- und Szenarioanalysen wie thematische oder länderspezifische Startup- und Business-Landscapes oder das automatisierte Beobachten der wissenschaftlichen Publikationslandschaft mittels Algorithmen zur Verarbeitung natürlicher Sprache (Natural Language Processing, NLP) detektiert das Team sogenannte emerging disruptive technologies (EDTs) und positioniert die Cyberagentur als eine relevante Innovationsakteurin im Ökosystem.

Als Multiplikator stellt das Innovations- und Wissensmanagement das gewonnene Wissen für die Cyberagentur und die Bedarfsträger zur Verfügung, um es weiter verwendet zu können. Zudem ist das Innovations- und Wissensmanagement für die Konzeption und den Aufbau der bereichsübergreifenden Cyberagentur-Bibliothek „CyberThec“ zuständig, um den Cyberagentinnen und Cyberagenten einen ähnlich umfassenden Zugang zu vorhandenen Informationen, Forschungsergebnissen und Erkenntnissen zu ermöglichen, wie Nutzerinnen und Nutzern in großen Forschungseinrichtungen und an Hochschulen.

Im Jahr 2024 hat das Innovations- und Wissensmanagement gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik eine Startup Landscape Cyber–Bay Area erstellt und damit eine thematische Übersicht von amerikanischen Startup-Unternehmen in der Bay Area, die an forschungsintensiven Technologien im Bereich der Cybersicherheit arbeiten, generiert. Zudem hat das Team gemeinsam mit dem Referat Cybersicherheit durch KI und Cybersicherheit für KI eine Generative Künstliche Intelligenz Landscape erarbeitet, die europäische Unternehmen und Startups im Bereich Generative KI bündelt.

Derzeit arbeitet das Team an einer Foresight-Studie: Cybersicherheitslage der Zukunft in Deutschland mit dem Ziel, Szenarien verschiedener cyberspezifischer Gefährdungslagen, welche die zukünftige Cybersicherheit in Deutschland (in zehn bis 15 Jahren) maßgeblich beeinträchtigen können, darzustellen und Handlungsbedarfe abzuleiten. Durch die Analyse von Metadaten und Abstract-Texten wissenschaftlicher Veröffentlichungen beobachtet das Team zudem kontinuierlich Publikationslandschaften in relevanten Forschungsgebieten. So wird beispielsweise die Publikationsaktivität verschiedener Länder und Staatenbündnisse für verschiedene Forschungsgebiete quantifiziert. Weiterhin werden Schlagworte sowie Forschungskonzepte und -themen identifiziert, um Trends und relevante Entwicklungen im Wissenschaftsbereich abzubilden. Neben dem Netzwerk Trendanalyse, das Akteurinnen und Akteure aus der Trend- und Zukunftsanalyse im Bereich der Inneren und Äußeren Sicherheit zusammenbringt, leitet und betreut das Innovations- und Wissensmanagement seit 2024 auch den neu gegründeten Arbeitskreis für Wissensmanagement in (Cyber)Sicherheitsbehörden.

WISSENSCHAFTLICHER DIENST

Der Bereich Wissensmanagement soll sowohl das vorhandene Wissen innerhalb der Cyberagentur bündeln und verständlich für alle bereitstellen, als auch extern die Behörden und Organisationen mit Sicherheitsaufgaben mit spannendem Wissen versorgen.

Aufgebaut wurde und fortlaufend verbessert wird ein internes Innovations- und Wissensökosystem, das Cyberagentinnen und Cyberagenten zu Themen, Trends und Szenarien untereinander oder mit externen Akteurinnen und Akteuren diskutieren lässt. Dies erfolgt beispielsweise in Form von Interviews, Workshops oder Vortragsreihen. Auf diese Weise soll ein weiterer Zugriff auf die Ideenlandschaft der Cyberagentur und ihrer Umgebung erfolgen.

Das externe Wissensmanagement beschäftigt sich mit der Entwicklung einer innovativen Wissensplattform zur Verwertung von (Forschungs-)Ergebnissen der Cyberagentur. Hierfür wurden mittels gängiger Methoden Erfolgsfaktoren, Trends, Bedarfe, Ausrichtungen und Anwendungsszenarien ermittelt. Bisherige Vorarbeiten zeigen zentrale Herausforderungen und Möglichkeiten in den Handlungsfeldern der datengeleiteter Aggregation von Cyberwissen, der Verfügbarkeit von aktualisierten Informationen und Nachrichtengewinnung, dem sicheren Austausch von sensiblen Informationen sowie dem Bedarf Cyberwissen behördenübergreifend nutzen zu können. Auf Grundlage dessen wurden Use-Cases und Umsetzungsideen für eine mögliche Wissensplattform erstellt und entwickelt.

Für weitere Informationen steht das Innovations- und Wissensmanagement des Wissenschaftlichen Diensts der Cyberagentur zur Verfügung.
Kontaktieren Sie uns gerne unter:

innovationsmanagement@cyberagentur.de

cyberagentur

IdeenLab
Sicherheit der Zukunft

Auftrag:

Im Netzwerk die Knotenpunkte bilden

Der Auftrag des Verbindungswesens der Cyberagentur ist es, Bedarfe und Themen der Inneren und Äußeren Sicherheit zu ermitteln, die Kontakte der Agentur zu knüpfen und zu pflegen und als Anlaufstelle – Single Point of Contact (SPoC) – für Partner im behördlichen Ökosystem zu dienen. Dabei liegt ein besonderer Schwerpunkt auf der Kommunikation und Koordination der Zusammenarbeit mit den Behörden der Inneren und Äußeren Sicherheit.

Ein wesentlicher Baustein des Aufgabenbereichs des Verbindungswesens ist die Entwicklung, Gestaltung und Pflege von Verbindungen zu Organisationen, Gruppen oder Personen, die für die Cyberagentur und ihren Auftrag bedeutsam sind. Dazu gehört, potenzielle Jurymitglieder oder fachliche Ansprechpartner zu identifizieren, Kommunikationskanäle zu etablieren oder aufrecht zu erhalten, ein positives Image der Cyberagentur aufzubauen und Vertrauen zu schaffen. Die Teilnahme an relevanten Netzwerkveranstaltungen oder Konferenzen, die zur Vertiefung der Beziehungen dienen, ist ebenso ein wesentlicher Auftrag. Außerdem wird dort durch Fachvorträge aus den Streitkräften ein aktuelles Lagebild der Bedürfnisse der Bundeswehr vermittelt.

Um diesem Auftrag gerecht zu werden und die Bedarfsträger effektiv zu befähigen, werden durch das Verbindungswesen der Cyberagentur sogenannte IdeenLabs umgesetzt. Diese dienen der Identifizierung zukünftiger Themen (Fokus: 10-15 Jahre in der Zukunft) deutscher Sicherheitsbehörden und der Bundeswehr.

Die ersten Workshops wurden am 23. und 24. April 2024 in enger Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der BWI GmbH durchgeführt. Das Workshopformat zielt darauf ab, Fachleuten und Endanwenderinnen und Endanwendern aus dem operativen Bereich eine Stimme in der Ideenfindung der Cyberagentur zu geben und die Möglichkeit zu eröffnen, gemeinsam neue Forschungsimpulse zu generieren. Zusätzlich soll Endanwenderinnen und Endanwendern sowie Expertinnen und Experten aus dem operativen Geschäft ein grundlegendes Verständnis für Zukunftsdenken und die Bedeutung von Vorausschau in der Cybersicherheit vermittelt werden. Durch das interaktive Format und zielgerichtete Diskussionen werden Teilnehmerinnen und Teilnehmer dazu animiert, über den aktuellen Stand der Technik hinauszudenken.

Um in den IdeenLabs eine Vielzahl origineller und vor allem disruptiver Ideen zu generieren, wird eine Mischung aus verschiedenen Methoden wie Brainwriting und Design Thinking angewandt. Besonders Brainwriting gilt als effektive Methode zur Ideenfindung und ist speziell darauf ausgelegt, die kollektive Kreativität von Gruppen zu nutzen und gleichzeitig einige der häufigsten Einschränkungen herkömmlicher Brainstorming-Techniken zu überwinden. Die erarbeiteten Ideen werden anschließend im Rahmen von 1-minütigen „Mini-Pitches“ vorgestellt und die „disruptivsten“ Ideen gekürt. Die erarbeiteten Projektideen werden in den Ideenpool der Cyberagentur eingespeist und bilden somit eine Grundlage für zukünftige Projekte der Cyberagentur.

Der Rahmen der teilnehmenden Institutionen soll nun graduell im gesamten behördlichen Ökosystem der Inneren und Äußeren Sicherheit erweitert werden. Die Workshops sind ergebnisoffen und nicht thematisch fokussiert. Dabei ist es auch möglich, Workshops mit spezifischen Schwerpunkten umzusetzen, um zum Beispiel Themen oder Ideen aus dem F&I-Bereich weiterzuentwickeln.

Am 15. und 16. November 2023 fand in Halle (Saale) das 3. Netzwerktreffen der Innovationslabore der Polizeien statt. Mit den Schwerpunkten neue Technologien für die Polizei, digitale Transformation und Cybersicherheit bot das Treffen nicht nur einen relevanten thematischen Rahmen, sondern schuf auch mit verschiedenen, innovativen Formaten den perfekten Raum für Networking und fachlichen Austausch.

Nachdem das Innolab der Polizei Sachsen die Initiative im Jahr 2021 startete, übernahm im folgenden Jahr das Innovation Lab des Landesamtes für Zentrale Polizeiliche Dienste (LZPD) NRW den Staffelstab. Im vergangenen Jahr wurde die Veranstaltung dann durch die Cyberagentur mit inhaltlicher Unterstützung durch das Innolab der Polizei Sachsen umgesetzt. Ziel der Veranstaltung ist es, den Austausch und die Zusammenarbeit zwischen verschiedenen (polizeilichen) Innovationsakteuren auf Bund- und Länderebene zu fördern.

Innovatives Denken braucht innovative Formate

Am ersten Veranstaltungstag boten Poster-Sessions eine dynamische und interaktive Alternative zu herkömmlichen Vorträgen und schufen eine informelle Atmosphäre, die es den Teilnehmerinnen und Teilnehmern ermöglichte, ein breites Spektrum an innovativen Projekten kennenzulernen. Die Breite der vorgestellten Projekte und das Format selbst fanden großen Anklang und ermöglichten den Teilnehmerinnen und Teilnehmern, zahlreiche neue Projekte zu entdecken.

Vorstellung des „Streifenwagens der Zukunft“

Ein Highlight der Veranstaltung war die Präsentation des „Streifenwagens der Zukunft“ durch das Innolab des LZPD NRW. Das Konzeptfahrzeug, in welchem innovative Einsatztechnik getestet wird, enthält unter anderem einen Bordcomputer mit Echtzeit-Lageinformationen, eine Vielzahl integrierter Kameras zur Geschwindigkeits- und Abstandsmessung und sensorbasiertes Blaulicht.

Visionen greifbar machen mit Lego® Serious Play®

Am zweiten Veranstaltungstag wurde ein Lego® Serious Play® Workshop durchgeführt, in welchem die Teilnehmerinnen und Teilnehmer strukturiert Ideen zu den Themen „Streifenwagen der Zukunft“ und „Polizist/Polizistin der Zukunft“ erarbeiteten. Ziel hierbei war es sowohl eine neue Methodik und die vielfältigen Einsatzmöglichkeiten in Sicherheitsbehörden zu vermitteln als auch Zukunftsbedarfe und neue Themen zu identifizieren.

Die vielen vereinbarten Folgeaustausche und die positive Resonanz der Teilnehmerinnen und Teilnehmer verdeutlichten den Erfolg und die Bedeutung des Treffens. Die engagierte Teilnahme und der Austausch von Projekten und Ideen zeigten, dass der Weg für eine enge und zukunftsorientierte Zusammenarbeit zwischen den Innovationslaboren und der Cyberagentur erfolgreich geebnet wurde.

Durch diese verbesserte Zusammenarbeit konnten wichtige Synergien geschaffen werden. Zusätzlich erwies sich die Erarbeitung neuer Themen und Zukunftsbedarfe als äußerst fruchtbar, um solide Grundlagen für die Entwicklung neuer Projekte zu schaffen.

Ausblick

Seine Fortsetzung findet das Netzwerktreffen der Innovationslabore im Dezember 2024 in Hannover. Die diesjährige Edition wird als Kooperation von Cyberagentur und dem Innovationslabor der Polizei Niedersachsen umgesetzt und soll sich neben innovativen Methoden auch mit dem Einsatz von KI für die Polizei befassen. Zusätzlich richtet die Cyberagentur im Oktober ein Netzwerktreffen für die Innovationseinheiten der Bundeswehr aus.

WISSENSCHAFTLICHER DIENST

Netzwerktreffen der Innovationslabore

Weitere Informationen: netzwerktreffen@cyberagentur.de

FORSCHUNG UND INNOVATION

ABTEILUNG SICHERE GESELLSCHAFT

- Cyberresiliente Gesellschaft
- Mensch-Maschine-Interaktion
- Digitale Identitäten
- Cyberbefähigter Staat

Interdisziplinär inspiriert, visionär gestaltet, innovativ umgesetzt

Als Abteilung „Sichere Gesellschaft“ legen wir den Schwerpunkt auf die Zukunftssicherheit der Gesellschaft im Zeitalter rasanter Technologieentwicklungen. Unser Ziel ist es, die sozialen und ethischen Auswirkungen neuer Technologien zu verstehen und aktiv mitzugestalten, um eine sichere und resiliente digitale Welt zu fördern. Dabei treiben wir technologische Innovationen voran und analysieren deren Einflüsse auf die Gesellschaft.

Im Referat Cyberresiliente Gesellschaft haben wir uns bis dato u.a. mit Cyberkriminalität, Fragen der Resilienz und Desinformation beschäftigt. Unser Ziel ist es, disruptive Forschung anzustoßen, um Strafverfolgungsbehörden im Kampf gegen Cyberkriminalität zu unterstützen und zu stärken. Dabei sollen auch Maßnahmen entwickelt werden, die zur Cybersicherheit und Resilienz der gesamten Bevölkerung beitragen. Für die Entwicklung von Ideen zu möglichen zukünftigen Technologien beschäftigen wir uns mit aktuellen Trends und der Beeinflussung von Menschen durch Fake News. So wollen wir zum Beispiel wissen, wie Desinformation erkannt, analysiert und verhindert werden kann. Die Cyberresiliente Gesellschaft stellt den Faktor Mensch in den Mittelpunkt aller Betrachtungen.

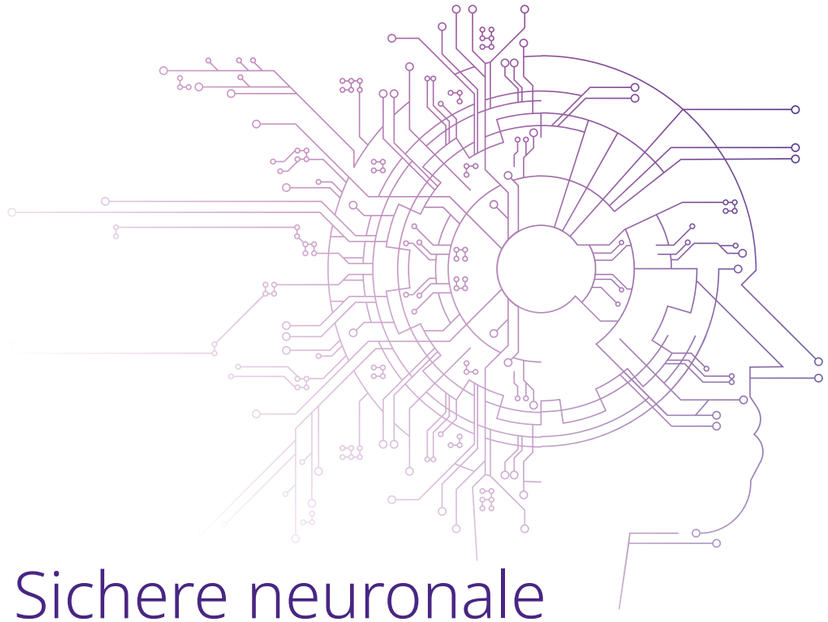
FAKTOR MENSCH IM MITTELPUNKT

Im Referat Mensch-Maschine-Interaktion tauchen wir tief in die Welt der Zukunftstechnologien ein. Hier arbeiten wir daran, das Zusammenspiel zwischen Mensch und Maschine zu revolutionieren. In einem laufenden Forschungsprojekt wird an der Entwicklung eines neuen Prototypen gearbeitet, der es ermöglichen soll, dass Menschen mit Hilfe ihrer Gedanken eine Maschine steuern können. Doch auch weitere und neuere Formen der Mensch-Maschine-Interaktion sind für uns spannend: So beschäftigen wir uns neben den klassischen Gehirn-Computer-Schnittstellen mit XR-Technologien und dem Einfluss von KI auf die Gesellschaft.

Im Referat Digitale Identitäten steht die sichere Authentifizierung der Menschen im digitalen Zeitalter im Fokus. Hier beschäftigen wir uns mit der Frage, wie Individuen ihr digitales Ich erstellen, steuern und verwalten können. Um dem nachzugehen, lassen wir neue biometrische Verfahren entwickeln, mit denen sich Nutzerinnen und Nutzer zukünftig sicher authentifizieren können. Betrachtet werden sollen dabei auch die Erwartungen von Menschen an diese neuen Technologien, um sicherstellen zu können, dass die Bedürfnisse und Ängste im Blick behalten und für zukünftige Entwicklungen in dem Bereich berücksichtigt werden.

Im Mittelpunkt des Referats Cyberbefähigter Staat steht die Fragestellung, wie Cyberkriminalität erkannt und bekämpft werden kann, um den Staat und die Gesellschaft effektiv gegen Cyberangriffe zu schützen. Konkret lassen wir erforschen, wie bei der Verwendung von KI-Systemen eine sichere Beweisführung möglich ist, wie der Aufnahmeort aus Audiodateien rekonstruiert werden kann und wie anhand eines einheitlichen forensischen Datenformats neue Ermittlungshinweise ableitbar sind. Wichtig ist uns dabei, neue Methoden zu entwickeln, die eine gerichtsfeste Erfassung, Analyse und Auswertung forensischer Daten ermöglichen.

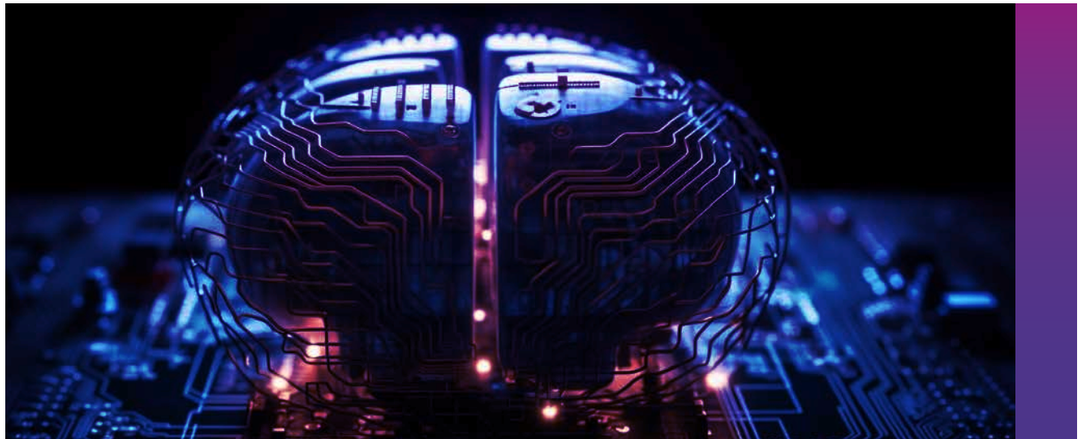
Bei all diesen umfangreichen und komplexen Themen können wir auf ein interdisziplinäres Team zurückgreifen, das sich aus Menschen verschiedenster Fachrichtungen zusammensetzt. Von Natur- über Rechts- bis hin zu Geisteswissenschaftlern, bei uns fließen unterschiedlichste Perspektiven zusammen. Auch über die Fachgrenzen der Referate hinaus tauschen wir uns regelmäßig über Anforderungen, Chancen und Gefahren zukünftiger Entwicklungen aus. Denn nur so können wir sicherstellen, dass auch in Zukunft verantwortungsvolle Technologien entwickelt werden, die ihren Teil für die Sicherheit der Gesellschaft beitragen.



Sichere neuronale Mensch-Maschine-Interaktion (BCI)

BCI Vorstudie

Das Projekt „Sichere neuronale Mensch-Maschine-Interaktion“ bringt Brain-Computer-Interfaces (BCIs) auf ein neues Level der Sicherheit. BCIs sind revolutionäre Technologien, die es ermöglichen, elektrische Signale aus dem Gehirn auszulesen und damit externe Geräte zu steuern. So können Querschnittsgelähmte bspw. lernen, einen Roboterarm mit ihren Gedanken zu steuern. Doch viele Neurotechnologien müssen aktuell noch invasiv implantiert werden, d.h. man muss die Schädeldecke eines Menschen öffnen und die Elektroden direkt auf die Gehirnoberfläche oder in tieferen Regionen einsetzen. Um das zu vermeiden, möchten wir eine Neurotechnologie entwickeln lassen, die ohne invasive Methoden funktioniert. Dabei ist es für uns von besonderer Bedeutung, die Sicherheit und den Schutz persönlicher Nutzerdaten zu sichern. Um die Persönlichkeitsrechte und die Datensicherheit bei neuronaler Mensch-Maschine-Kommunikation zu gewährleisten, haben wir das Brain-Privacy-Framework entwickeln lassen. Darin wird beschrieben, wie Neurotechnologie sicher und verantwortungsvoll entwickelt werden kann und die Nutzerinnen und Nutzer ein hohes Maß an Kontrolle über ihre Daten behalten. Das Brain-Privacy-Framework setzt damit neue Maßstäbe für Sicherheit und Verantwortung in der Entwicklung neuer BCI-Technologie.



Nach der erfolgreichen BCI-Vorstudie sind wir mit BCI Stufe 2 einen Schritt weitergegangen und haben die Entwicklung eines Prototypen für ein sicheres Brain-Computer-Interface (BCI) in Auftrag gegeben. Nach umfangreicher Prüfung und intensiven Verhandlungsrunden konnte sich das Projekt „Neuroadaptivität für autonome Systeme“ (NAFAS) vom Cottbuser Startup Zander Laboratories GmbH gegen die Mitbewerberinnen und Mitbewerber durchsetzen. Eine öffentlichkeitswirksame Vertragsunterzeichnung fand Mitte Dezember 2023 statt.

BCI Stufe 2

Der Geschäftsführer und Projektleiter von NAFAS, Prof. Dr. Thorsten Zander, sieht den Forschungsauftrag als große Chance, um eigene Impulse in der Neurotechnologie zu setzen: *„Der Forschungsauftrag wird es uns erlauben, Technologien aus dem Labor näher in die Realität zu bringen. Des Weiteren können Fragen beantwortet werden, die bisher aus Mangel an Forschungsgeldern nicht angegangen werden konnten, obwohl sie extrem wichtig und weitreichend sind.“*

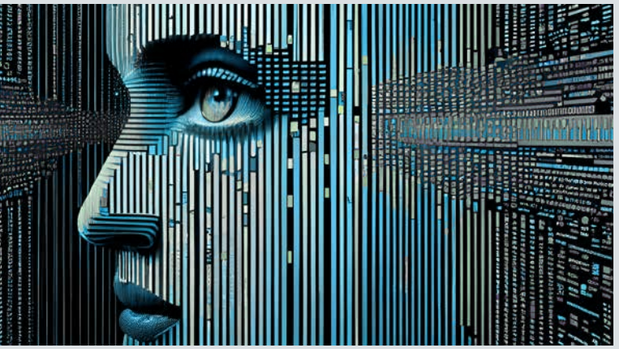
Das Herzstück von NAFAS besteht aus der Verwendung von Neurotechnologie, die es ermöglicht, Informationen von einem Gehirn auszulesen und so die Interaktion zwischen Mensch und Maschine zu erleichtern. Dabei wird erstmalig mit sogenannten passiven BCIs gearbeitet. Mit einem passiven BCI muss sich die Nutzerin oder der Nutzer im Gegensatz zu herkömmlichen Ansätzen in den Neurotechnologien nicht aktiv bestimmte Dinge vorstellen, sondern – wie man es im Alltag auch gewohnt ist – einfach die gewünschte Handlung durchführen. Ziel ist es, eine neue Generation von Maschinen zu entwickeln, die sich in Echtzeit an die kognitiven und affektiven Zustände der Benutzerin oder des Benutzers anpassen können, um das Erlebnis zu personalisieren und die Effektivität autonomer Systeme zu verbessern. *„Ich habe das Forschungsfeld der passiven Brain-Computer-Interfaces ab dem Jahr 2008 eingeleitet und seitdem intensiv untersucht.“*, fasst Zander seinen Werdegang zusammen, *„Insbesondere ist hier hervorzuheben, dass wir in einer ersten Untersuchung bewiesen haben, dass eine KI wirklich direkt vom menschlichen Gehirn lernen kann.“* Vor dem Hintergrund der passiven Neurotechnologie wird sich Zander Labs die nächsten 4 Jahre mit der Entwicklung eines Prototypen beschäftigen. Dieser soll dazu in der Lage sein, Informationen von einem Gehirn auszulesen, so dass eine Person über ihre Gedanken mit einem externen System Informationen austauschen, es kontrollieren oder sogar steuern kann. Wenn das gelingt, können Mensch und Maschine über das BCI gemeinsam Handlungen ausführen, Ziele verfolgen und Informationen austauschen. Zander erhofft sich davon, künstliche und menschliche Intelligenz näher zusammenzubringen:

„Auf diese Weise wird dann unsere Kommunikation mit Maschinen revolutioniert werden, indem diese eher implizit geschieht und wir nicht mehr alles mühsam, über Tastatur und Maus, in die Sprache der Maschinen übersetzen müssen. Die Maschinen entwickeln dadurch so etwas wie eine Intuition, oder sogar eine Empathie. Das resultierende bessere Verständnis, was die Maschinen für den Menschen entwickeln, wird dazu führen, dass KIs generell sicherer und hilfreicher werden.“

Um dieses Ziel zu erreichen, arbeitet die Zander Laboratories GmbH eng mit renommierten Institutionen zusammen - wie dem Fraunhofer Institut für Digitale Medientechnologie (IDMT), der TNO in den Niederlanden, KiviCore GmbH aus Dresden, Eaglescience Software B.V. in Haarlem sowie akademischen Einrichtungen der Brandenburgischen Technischen Universität Cottbus-Senftenberg, der Universität Wien und der Julius-Maximilians-Universität Würzburg. Von den vier Jahren Gesamtlaufzeit hat das Konsortium bereits die ersten sechs Monate der Projektlaufzeit abgeschlossen.

Die Herausforderungen, vor denen das Team seit der Erteilung des Forschungsauftrags steht, fasst Zander folgendermaßen zusammen: *„Momentan war das größte Problem, genügend Talente zu finden, die uns bei dem Projekt helfen können. Einerseits haben wir über 950 Bewerbungen auf unsere ausgeschriebenen Stellen, was natürlich gut ist, aber auch eine intensive Auswahl verlangt hat. Des Weiteren haben wir Zeit damit verbracht, uns mit den unterbeauftragten Partnern aus Wissenschaft und Industrie darauf zu einigen, wie wir zusammen die Problemstellungen angehen werden. Wir sind jedoch enorm zufrieden mit dem Fortschritt und freuen uns sehr auf die nächsten Schritte!“.*

Seit dem offiziellen Start begleitet die Cyberagentur das NAFAS-Projekt mit regelmäßigen virtuellen und persönlichen Treffen. Wir blicken weiterhin gespannt auf die Zukunft von NAFAS und freuen uns auf die ersten Ergebnisse.



Forensik Intelligenter Systeme (FIS)

Durch den globalen Einsatz intelligenter Systeme wächst die Bedrohung durch falsches KI-Verhalten stetig. Beispiele für komplexe KI-Systeme sind Large Language Models (LLMs) wie der Suchassistent Copilot, der Chatbot ChatGPT und KI-Systeme zur Generierung realistischer Bilder wie DALL-E 2. Um besser zu verstehen, wann und warum diese KI-Systeme versagen, müssen wir forensische Methoden anwenden.

Unser Projekt „Forensik intelligenter Systeme“ (FIS) zielt darauf ab, komplexe KI-Systeme, wie autonome Fahrzeuge, umfassend auszuwerten. Diese Auswertung soll forensischen und kriminalistischen Standards entsprechen, sodass sie als Beweis vor Gericht dienen kann. Wir möchten nachvollziehen können, wie Straftaten mit KI-Systemen als Werkzeug oder Ursache begangen wurden, z. B. durch autonome Robotik in sicherheitskritischen Produktionsketten. Derzeit können wir Ursachen wie absichtliche Code-Manipulation, Hardware- und Softwarefehler oder falsche Bedienung noch nicht eindeutig unterscheiden, da die Komplexität der Algorithmen und die Anzahl der Parameter zu hoch sind.

Eine zusätzliche Herausforderung stellen kontinuierlich lernende KI-Systeme dar, die ihre Parameter ständig anpassen oder überschreiben. Ein bekanntes Beispiel sind autonome Fahrzeuge, deren Vernetzung sie anfälliger für Angriffe macht. Um diese Risiken zu minimieren, müssen wir Manipulationen frühzeitig erkennen. Maßnahmen zur Digital Forensic Readiness (DFR) sind entscheidend für den Erfolg autonomer Fahrzeugsysteme.

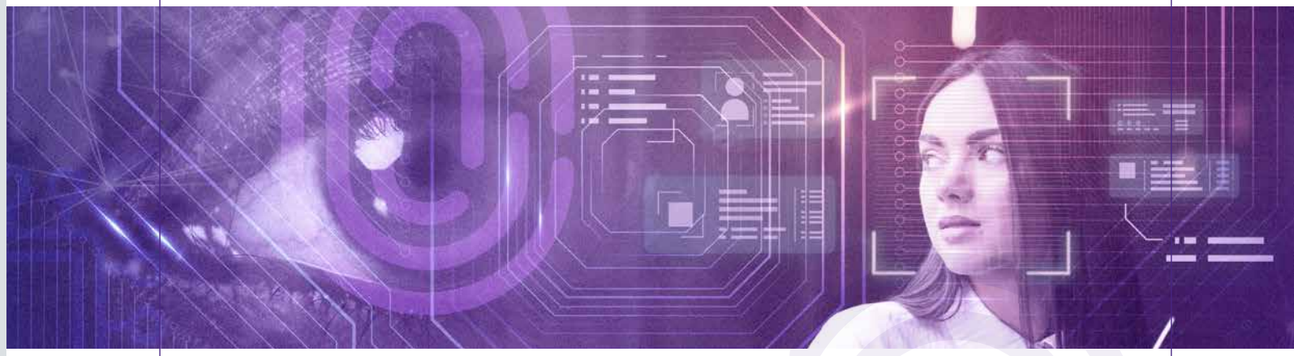
Unser Projekt FIS unterscheidet sich von aktuellen Ansätzen zur Erklärung der Entscheidungsfindung künstlicher Intelligenz (EXplainable AI). Während XAI-Methoden darauf abzielen, verständliche KI-Systeme zu entwerfen und den Entscheidungsprozess offenzulegen, fokussieren wir uns auf forensische Nachweise für beliebig komplexe KI-Systeme aus der Gruppe der tief neuronalen Netzwerke (DNN). XAI eignet sich zur Untersuchung der mathematischen Funktionsweise von KI, nicht aber für die vollständige forensische Auswertung komplexer Blackbox-KI-Modelle. Bisher gibt es keine transparenten und auditierbaren Lösungen für diese Probleme, was unser Projekt technisch, wirtschaftlich und gesellschaftlich relevant macht.

Unser Forschungsprojekt ist in fünf Bereiche aufgeteilt. Der erste Bereich untersucht den Ist-Stand aktueller Methoden zur Nachweisführung von KI-Entscheidungen und dient als Basis für die weiteren Forschungsfragen. Dieser Bereich wird von allen Teilnehmerinnen und Teilnehmern parallel bearbeitet. Die Bereiche zwei bis vier beschäftigen sich mit der Anwendung dieser Methoden auf „Autonome Systeme“, „Text- und Audioverarbeitung“ und „Bild- und Videoverarbeitung“.

Dabei soll das KI-System ein neuronales Netzwerk mit mindestens drei Schichten und kontinuierlich lernendem Verhalten aufweisen. Ziel des Projektes sind Methoden, um Angriffe wie Evasionsangriffe, Data-Poisoning-Angriffe, Inversionsangriffe und Datenrekonstruktion gerichtsfest nachzuweisen. Der fünfte Bereich befasst sich mit der Einhaltung rechtlicher Voraussetzungen, um sicherzustellen, dass die entwickelten Methoden vor Gericht anwendbar sind.

Unser Projekt hat eine hohe Relevanz für die Strafverfolgung in Deutschland. Es besteht großes Interesse seitens der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS), unsere Ergebnisse weiterzuentwickeln. Die Erkenntnisse könnten vom Bundeskriminalamt (BKA), der Bundespolizei (BPol) und den deutschen Nachrichtendiensten genutzt werden.

Auch das Zentrum für Cybersicherheit der Bundeswehr (ZCSBw) betont die Bedeutung unseres Projekts.



Digitale Authentifizierung durch neuartige biometrische Verfahren (AuBi)

Die Gesichtserkennung zum Entsperren des Laptops oder der Fingerabdruck zum Zugriff auf das Online-Konto – viele Menschen verwenden es bereits, ohne sich dessen bewusst zu sein: Biometrische Verfahren, mit denen sie sich ohne Eingabe eines Passworts als legitime Nutzerin oder legitimer Nutzer authentifizieren können. Wir möchten nun den nächsten Schritt gehen und mit dem Projekt „Digitale Authentifizierung durch neuartige biometrische Verfahren“ (AuBi) Technologien entwickeln, die in Zukunft für die Authentifizierung von Personen genutzt werden können. Insgesamt soll das Projekt sowohl technisch als auch gesellschaftlich neue Standards für die digitale Authentifizierung setzen. Dabei ist uns besonders wichtig, die Technologie sicher zu entwickeln und verantwortungsvoll mit den sensiblen Daten der Nutzerinnen und Nutzer umzugehen. Um dieser Vision näher zu kommen, haben wir drei spannende Themenfelder identifiziert: Verhaltensbiometrie, stimulus-induzierte Biometrie und universelle Muster.

Bei der Verhaltensbiometrie werden individuelle Verhaltensweisen aufgezeichnet, wie das Gangbild oder das Tippen auf einem Smartphone. Daraus entstehende Muster können zur kontinuierlichen Authentifizierung genutzt werden. Damit kann sichergestellt werden, dass sich auch wirklich die richtige Nutzerin oder der richtige Nutzer vor dem jeweiligen Endgerät befindet. Darüber hinaus können Geräte wie Smartphones oder Tablets sofort gesperrt werden, wenn sie in die Hände Unbefugter gelangen.

Bei der stimulus-induzierten Biometrie handelt es sich um ein Verfahren, bei dem ein spezifischer Reiz ausgesendet wird, bspw. ein Ton oder ein visueller Eindruck. Der Nutzer reagiert darauf mit einer individuellen körperlichen Reaktion. Das Paar aus gesendetem Reiz und der Reaktion der Nutzerin oder des Nutzers kann dann eine sichere Authentifikation ermöglichen. Diese Methode verspricht hohe Sicherheit gegen Manipulationen und Datendiebstahl.

Bei universellen Mustern wird auch ein bestimmter Reiz ausgesendet, auf den die Nutzerin oder der Nutzer auf eine bestimmte Art und Weise reagiert. Allerdings wird hier der Reiz individuell an die Person angepasst und eine Reaktion ausgelöst, die bei allen Menschen gleich ist. Damit entsteht ein universelles Muster, das über Personengruppen hinweg gleich ist. Dieser Forschungsschwerpunkt ist sehr experimentell und wenig erforscht, damit aber besonders spannend und interessant für zukünftige, mögliche Technologien.

Cyberkriminalität

Forschung zu zukünftiger Cyberkriminalität (zCK)

Unser Forschungsprojekt „zCK“ nimmt die Zukunft der Cyberkriminalität ins Visier. Es besteht aus zwei spannenden Bereichen: „Mustererkennung und -analyse“ und „Zukunftsanalyse“

Bei „Mustererkennung und -analyse“ geht es darum, globale Entwicklungen der Cyberkriminalität frühzeitig zu erkennen. Mit Hilfe von neuartiger Mustererkennung wollen wir herausfinden, welche Ziele, Taktiken und Methoden Cyberkriminelle weltweit nutzen. Ziel ist es, ein Frühwarnradar zu entwickeln, das nicht nur technische Faktoren, sondern auch kulturelle und strukturelle Besonderheiten verschiedener Länder berücksichtigt. So können wir nationale und internationale Entwicklungen im Bereich der Cyberkriminalität besser voraussehen und entsprechend reagieren.

Der Bereich „Zukunftsanalyse“ konzentriert sich darauf, wie sich Cyberkriminalität in den nächsten fünf bis 15 Jahren durch technologische Veränderungen in Deutschland entwickeln könnte. Mithilfe von Methoden wie Trend- und Szenarioanalysen wollen wir vorhersagen, welche Technologien die Cyberkriminalität beeinflussen können. Auch hier fließen kulturelle und strukturelle Bedingungen Deutschlands ein, um ein umfassendes auf Deutschland zugeschnittenes Bild zu erhalten.

Für das Projekt wurden bereits mehrere Bewerberinnen und Bewerber ausgewählt, die im Sommer ihre Ideen skizziert haben. Im Herbst startet die ausführliche Konzeptphase, für die drei besten Teams pro Teilprojekt. Am Ende wird jeweils eine Auftragnehmerin oder ein Auftragnehmer ausgewählt, der das Projekt in der Umsetzungsphase durchführt.

Schäden durch Cyberkriminalität (SCK)

Unser Projekt „SCK“ legt einen weiteren Grundstein für den Schwerpunkt „Cyberresiliente Gesellschaft“ der Cyberagentur

Ziel der Forschung ist die Entwicklung eines Modells samt Metriken und Methodiken, das kurz-, mittel- und langfristige materielle sowie immaterielle Schäden und Kaskadeneffekte durch Cyberkriminalität systematisch, reproduzierbar und überprüfbar erfasst. Das Modell soll robust gegenüber Veränderungen der Kriminalitätslandschaft sein, um auch zukünftige Formen von Cyberkriminalität frühzeitig bewertbar zu machen. Mit diesem evidenzbasierten Ansatz wollen wir ein Werkzeug zur Analyse und Einschätzung der Auswirkungen solcher Straftaten auf Gesellschaft, Wirtschaft und Staat schaffen. Langfristig soll dies die polizeistrategische und gesetzgeberische Ausrichtung unterstützen und dabei helfen, Ressourcen gezielt einsetzen zu können sowie die Cyberkriminalitäts- und Sicherheitsforschung zu stärken.

Um potenzielle Teilnehmerinnen und Teilnehmer zu vernetzen, fand im Mai 2024 ein Partnering-Event statt, bei dem auch zahlreiche internationale Interessierte teilnahmen. Die Ausschreibung des Forschungsvorhabens erfolgte am 26. Juni 2024 und im September startet die Kurzkonzeptphase.

Geeignete Bewerberinnen und Bewerber treten in der Kurz- und Langkonzeptphase in den Wettbewerb, denn nur das beste Team gelangt in die 42-monatige Umsetzungsphase. Mit diesem Projekt können die Auswirkungen von Cyberkriminalität besser verstanden und eine cyberresiliente Gesellschaft gefördert werden.

ABTEILUNG SICHERE SYSTEME

Schutz Kritischer Infrastrukturen

Cybersicherheit der Bundesverwaltung und der Streitkräfte

Cybersicherheit in schwierigen Umgebungen

Sichere Hardware und Lieferketten

Wegweisende Sicherheitsforschung für Sichere Systeme

Die Abteilung „Sichere Systeme“ ist ein integraler Bestandteil des Forschungs- und Innovationsbereichs der Cyberagentur. Sie setzt sich aus den Referaten „Schutz Kritischer Infrastrukturen“, „Cybersicherheit der Bundesverwaltung und der Streitkräfte“, „Cybersicherheit in schwierigen Umgebungen“ und „Sichere Hardware und Lieferketten“ zusammen. Das Hauptziel dieser Abteilung ist es, staatliche Institutionen und Betreiber Kritischer Infrastrukturen dabei zu unterstützen, ihre komplexen Systeme sicherer, resilienter und effektiver zu betreiben.

Im Rahmen dieser Zielsetzung initiiert und begleitet die Abteilung Forschungsprojekte im Bereich der Cybersicherheit. Der besondere Fokus liegt auf vernetzten, physischen und digitalen Systemen und Infrastrukturen. Zentrale Forschungsfragestellungen beschäftigen sich dabei mit der Verifikation von Sicherheitseigenschaften in zukünftigen Systemen, insbesondere an den Schnittstellen zwischen Hardware und Software. Hierbei geht es darum, Methoden und Werkzeuge zu entwickeln, die beweisbare und garantierte Sicherheitseigenschaften bereits während der gemeinsamen Entwicklung sicherstellen können.

Ein weiteres wichtiges Thema ist die Absicherung sicherheitskritischer und systemrelevanter Infrastrukturen und Organisationen. Die Abteilung untersucht neuartige Ansätze zur Absicherung existierender und zukünftiger Systeme sowie die Fähigkeiten, die für die Prävention, Detektion, Reaktion und Attribution im Hinblick auf existenzbedrohende Risiken aus dem Cyber- und Informationsraum notwendig sind.

Die Abteilung beschäftigt sich auch mit der Entwicklung neuartiger Rechnerarchitekturen, die den Anforderungen zukünftiger Anwendungen und Systeme gewachsen sind. Dabei stehen Themen wie Sicherheit, Verschlüsselung und Rechenleistung im Mittelpunkt, die angesichts des steigenden Ressourcenbedarfs und disruptiver Entwicklungen in der Kryptoanalyse und bei Quantensystemen besonders relevant sind.

Ein weiteres zentrales Forschungsgebiet ist die sichere und zuverlässige Kommunikation wesentlicher Informationen über ressourcenbeschränkte Verbindungen, wie beispielsweise Satelliten. Hierbei geht es darum, Kommunikationstechnologien zu entwickeln, die auch in schwierigen Umgebungen, wie dem Weltall oder unter Wasser, robust funktionieren und dabei sowohl Sicherheit als auch Zuverlässigkeit gewährleisten. Die spezifischen Herausforderungen im Bereich der Cybersicherheit in den Verwaltungsorganen des Bundes werden ebenfalls eingehend untersucht. Ziel ist es, praktikable Lösungen zur Bewältigung dieser Herausforderungen zu entwickeln.

Diese Themenbereiche spiegeln exemplarisch die Arbeit der Abteilung „Sichere Systeme“ wider, die stets im engen Austausch mit Ideengebern und Bedarfsträgern stattfindet. Von zentraler Bedeutung ist die Identifikation grundlegender Fragestellungen aus praktischen Problemen. Die wissenschaftliche Analyse und Bearbeitung dieser Fragestellungen erfolgt in den Fachreferaten und erstreckt sich über einen Zeithorizont von zehn bis 15 Jahren, wobei technologische Reifegrade von 1 bis 4 angestrebt werden.

Die Abteilung arbeitet abteilungs- und referatsübergreifend zusammen, um themenbasiert anspruchsvolle und risikobehaftete Leistungsbeschreibungen zu erstellen, die als Basis für die Beschaffung von Forschung und Entwicklung innovativer Lösungen dienen.

KRITIS
und die Risiken aus dem Cyber- und Informationsraum

IT-Infrastrukturen sind von zentraler Bedeutung für unsere Gesellschaft, wie im KRITIS-Dachgesetz und in der Cybersicherheitsstrategie hervorgehoben wird. Gezielte Angriffe auf diese Strukturen gefährden die Innere und Äußere Sicherheit erheblich.
Das Projekt „Existenzbedrohende Risiken aus dem Cyber- und Informationsraum – Hochsicherheit in sicherheitskritischen und verteidigungsrelevanten Szenarien“ (HSK) untersucht innovative Ansätze zum Schutz dieser Kritischen Infrastrukturen und nimmt dabei sowohl die Perspektive einzelner Systemelemente als auch deren Verbindungen in den Fokus.

Das Ziel des Forschungsauftrags ist es, neue Fähigkeiten für die operative Cybersicherheit zu entwickeln, damit deutsche Behörden besser auf zukünftige Bedrohungen im digitalen Raum vorbereitet sind. Die Forschung konzentriert sich auf vier zentrale Bereiche: Prävention, Detektion, Reaktion und Attribution von Cyberangriffen. Konkret sollen Grundlagenforschung und praktische Anwendungen in den Bereichen automatisierte Schwachstellenidentifikation in sicherheitssensiblen Systemen, Reaktion und Forensik während Cyberangriffen sowie die klare Zuordnung von Cyberangriffen entwickelt werden. Das Projekt zeichnet sich durch eine Kombination verschiedener Foschungssäulen aus, was vielfältige Ansätze und Methoden ermöglicht. Diese Vielfalt bietet den beteiligten Forschern zahlreiche Möglichkeiten, neue und disruptive Lösungen zu entwickeln.

Die erste Forschungsphase begann am 1. September 2023 und lief bis zum 31. August 2024. In dieser Phase waren folgende Projekte vertreten (in alphabethischer Reihenfolge):

Attribut, geführt von der Otto-von-Guericke-Universität Magdeburg, zielt darauf ab, Schadcodeangriffe unter realitätsnahen Bedingungen aufzuklären und zu attribuieren. Besonderes Augenmerk liegt auf der Nutzung verdeckter Kommunikation und steganographischer Kanäle. Stego-Malware infiltriert Netzwerke verdeckt, versteckt Command & Control-Kommunikation und exfiltriert Daten unerkannt. Das Projekt verfolgt Ziele wie die Charakterisierung steganographischer Verfahren, die Integration dieser Verfahren in forensische Modelle, die Messung des Auftretens von verdecktem Schadcode sowie die Modellierung der Detektion und Reaktion in Laborumgebungen.

Mantra, geleitet von der Asvin GmbH, entwickelt ein Framework zum Echtzeitaustausch von Cyberangriffsmustern und deren Risikomanagement. Der Ansatz basiert auf Graphen-Modellen und bietet erhebliche Vorteile im Cybersicherheitsmanagement, insbesondere bei der Automatisierung und Priorisierung von Maßnahmen zur Risikominimierung und Abwehr. Zu den Zielen gehören die automatisierte Informationsbereitstellung, der Austausch von Cybersicherheitswissen, die Aggregation von Wissen in einem verteilten System sowie die Erhöhung der Resilienz und Vertrauenswürdigkeit.

Sovereign, ein Projekt unter Federführung der Universität Hamburg, zielt darauf ab, eine souveräne Cyber-Defense-Plattform zu schaffen, die in bestehende Kritische Infrastrukturen integriert werden kann. Diese Plattform soll Infrastrukturen schützen, die aus vielen, teilweise unbekannten Komponenten bestehen. Zu den Zielen gehören die Entwicklung einer Zero-Trust Cyber-Defense-Plattform basierend auf offener Software und Hardware, das verteilte Monitoring von Netzen und Systemen, KI-basierte Methoden zur Erkennung und Attribution komplexer Angriffe sowie die dynamische Risikobewertung und das Business-Impact-Assessment laufender Angriffe.

Nach Abschluss der ersten Forschungsphase werden maximal zwei der drei Projekte in die zweite, dreijährige Forschungsphase übergehen. Dies markiert einen wichtigen Meilenstein für das Projekt HSK, da die Ergebnisse dieser Phase maßgeblich zur Stärkung der Nationalen Cybersicherheitsstrategien in Deutschland beitragen werden.

Die engagierte und innovative Arbeit der beteiligten Auftragnehmer ist entscheidend für die Entwicklung robuster und zukunftssicherer Lösungen im Bereich der Cybersicherheit.

Sichere IT-Zukunft:
Durchgängige Verifikation für robuste Systeme

Das Projekt „Ökosystem vertrauenswürdige IT“ (ÖvIT) hat das Ziel, Technologien, Methoden und Werkzeuge für vollständig formal verifizierte Software- und Hardwarekomponenten zu erforschen und zu entwickeln.

IT-Systeme werden zunehmend komplexer und dadurch anfälliger für sicherheitskritische Fehler. Viele der gefährlichsten Schwachstellen lassen sich auf wenige grundsätzliche Probleme zurückführen. Gängige Programmier- und Testmethoden sind in der Lage, viele Fehler in Hardware und Software zu vermeiden, doch sie entdecken nicht alle Schwachstellen. Hier kommt die sogenannte formale Verifikation ins Spiel: Diese mathematisch-logischen Methoden können nachweisen, dass ein IT-System vollständig frei von Sicherheitslücken ist, die vorher definierte Sicherheitseigenschaften verletzen würden. Dabei werden die gewünschten Sicherheitseigenschaften formal festgehalten und sowohl Hardware als auch Software so erstellt, dass die Erfüllung dieser Eigenschaften mathematisch beweisbar ist.

Diese Verfahren erfordern jedoch Spezialkenntnisse und viel Zeit selbst von erfahrenen Informatikerinnen und Informatikern. Die Anwendung formaler Methoden ist für die heutige komplexe Hard- und Software nicht einfach oder schnell umzusetzen. Derzeit werden formale Methoden getrennt für Hardware und Software angewendet und oft nur für einzelne Aspekte. Es gibt aktuell kein ganzheitliches Verfahren, das die korrekte Implementierung eines gesamten IT-Ökosystems nachweisen kann.

Zudem soll ein Ökosystem von Entwicklerinnen und Entwicklern sowie Nutzerinnen und Nutzern bei kommerziellen Anbietern etabliert werden. Forscherinnen und Forscher sollen die formale Verifikation perspektivisch automatisiert für komplexere Systeme einsetzbar machen. Diese Grundlagenforschung wird sich über einen Zeitraum von fünf bis zehn Jahren erstrecken und erst in einem Folgeprojekt abgeschlossen werden können.

Ein durchgängiger Ansatz soll größere Verbreitung finden, indem auf einfacher zu nutzende, automatisierte und modulare Methoden und Werkzeuge gesetzt wird. Ein wichtiger Aspekt ist das aktive Community-Building als Teil des Projekts. Das Forschungsprojekt ist aus wissenschaftlich-technologischer Perspektive höchst ambitioniert und risikobehaftet, da ein gemeinsames Verifikationsprojekt für komplexe Hard- und Software bisher noch nicht erfolgreich realisiert wurde. Bei Erfolg können gängige Sicherheitslücken in vielen IT-Systemen bereits während der Entwicklung geschlossen werden. Dies gilt sowohl für Standard-Bürosysteme als auch für gehärtete IT-Systeme, die in Kritischen Infrastrukturen und der nationalen Sicherheit eingesetzt werden. Ziel ist es, Systeme mit beweisbarer Cybersicherheit breit anzuwenden, sodass Sicherheitslücken gar nicht erst auftreten.

Gleichzeitig soll der Ansatz „Cybersicherheit by Design“ stärker verbreitet werden. Das neu gewonnene Wissen und das entstehende Ökosystem stärken die technologische Souveränität Deutschlands. Eine Beschaffungspolitik des Bundes, die diesen Ansatz als Anforderung formuliert, wäre ein starker Anreiz für IT-Anbieter, die Ergebnisse rasch in Anwendungen und Produkte zu transferieren.

Revolutionäre Rechnerarchitekturen:

Vorstudie zu zukünftigen Technologien

Eines der zentralen Forschungsthemen der Cyberagentur ist die Untersuchung Alternativer Rechnerarchitekturen, die über die traditionelle binäre Logik auf Basis von Halbleiterchips hinausgehen. Diese Erforschung ist notwendig, da die aktuellen Entwicklungen an physikalische Grenzen stoßen. Um weiterhin Fortschritte zu erzielen, müssen neue Ansätze entwickelt werden. Die derzeitigen Architekturen sind zudem nicht für alle Problemstellungen der Informationsverarbeitung optimal geeignet. Durch den Einsatz besser geeigneter Architekturen könnten neue Fähigkeiten insbesondere im Bereich der Sicherheit erschlossen werden. Diese neuen Architekturen könnten widerstandsfähiger gegen Angriffe sein und ein robusteres Rechensystem ermöglichen. Außerdem könnte der Bedarf an strategischen Rohstoffen, die für die Herstellung von Halbleiterchips benötigt werden, minimiert oder sogar eliminiert werden, was zur technologischen Unabhängigkeit beitragen würde. Ein weiterer Vorteil effizienterer Architekturen wäre die Reduzierung des hohen und konstanten Energiebedarfs von Computern und Rechenzentren. Damit könnte die Rechenleistung flexibler und nachhaltiger erbracht werden.

Die Forschung an alternativen Rechnerarchitekturen ist disruptiv, da sie die traditionellen Grenzen der Rechentechnik überschreitet und neue Wege der Informationsverarbeitung eröffnet. Sie integriert Disziplinen wie Physik, Chemie und Biologie mit der Informatik, um leistungsfähigere und effizientere Systeme zu entwickeln. Dieser interdisziplinäre Ansatz hat das Potenzial, die Art und Weise, wie wir über Rechner und ihre Anwendungen denken, grundlegend zu verändern. Um diese ambitionierten Ziele zu erreichen, hat die Cyberagentur das Gesamtprojekt „Alternative Rechnerarchitekturen“ (ARA) ins Leben gerufen, das aufgrund der Vielzahl an Architekturen in zwei Teile gegliedert ist. Der erste Teil besteht aus einer Vorstudie, die darauf abzielt, die verschiedenen Architekturen zusammenzustellen, zu vergleichen und mit den sicherheitsrelevanten Bedürfnissen unserer Bedarfsträger abzugleichen. Auf Basis der Vorstudie wird anschließend ein größerer Forschungswettbewerb zur detaillierten Erforschung der einzelnen Architekturen durchgeführt.

FORSCHUNG UND INNOVATION · SICHERE SYSTEME

Der Auftrag für die Vorstudie besteht darin, ein Rahmenwerk zu entwickeln, um die folgenden zentralen Forschungsfragen zu beantworten:

> **Wie können die aktuellen und zukünftigen Sicherheitsprobleme im Zusammenhang mit Computern gruppiert und abstrahiert werden?**

> **Wie können die verschiedenen Rechnerarchitekturen gesammelt, verglichen, klassifiziert und mit den Problemen abgeglichen werden?**

> **Was ist der aktuelle Stand der Forschung und der Forschungsfinanzierung für die verschiedenen Architekturen?**

Die Firma Capgemini hat den Zuschlag für diesen ersten Teil erhalten und im April 2024 mit der Arbeit begonnen. Diese Vorstudie läuft über neun Monate bis zum Ende des Jahres. Parallel dazu führt die Cyberagentur Seminare durch, um Forscherinnen und Forscher, die Industrie und Bedarfsträger im Rahmen eines Community Buildings zusammenzubringen.

Der zweite Teil des Projekts, eine größere Forschungsausschreibung, ist für 2025 geplant und wird unter anderem auf den Ergebnissen der Vorstudie und der Seminar-Workshops basieren.

Resiliente Lieferketten:

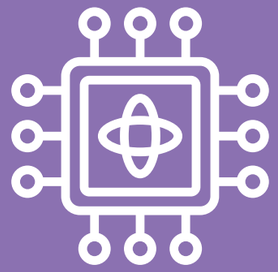
Schutz vor globalen Risiken

Die fortschreitende Globalisierung und Digitalisierung führen zu immer komplexeren und weniger transparenten Lieferketten sowie einer steigenden Abhängigkeit vom Ausland, insbesondere bei Hochtechnologie-Produkten wie Rüstungsgütern und Informationstechnologie für Sicherheitsbehörden und Kritische Infrastrukturen. Aufgrund dieser komplexen Abhängigkeiten wird es zunehmend schwierig, die Sicherheit und Zuverlässigkeit einer Lieferkette zu beurteilen. Wichtige Fragen betreffen die Resilienz einer Lieferkette bei einem Ausfall kritischer Zulieferer, die Möglichkeit gezielter Angriffe zur Unterbindung des Nachschubs und das Risiko, dass unfreundliche Akteure durch gezielte Unternehmenskäufe zu viel Einfluss gewinnen. Diese Fragen müssen im Interesse der nationalen Sicherheit vorausschauend beantwortet werden.

Um diese Herausforderungen zu bewältigen und mögliche Gegenmaßnahmen ergreifen zu können, sind zwei wesentliche Voraussetzungen notwendig. Erstens müssen die Lieferketten der öffentlichen Hand über die unmittelbaren Lieferanten hinaus bekannt sein, sowohl für materielle Güter als auch für Software und geistiges Eigentum. Zweitens muss es möglich sein, die Vielzahl der mittelbaren Lieferanten zu überwachen und automatisiert Hinweise zu erhalten, wenn sich bei den Eigentümern oder dem Schlüsselpersonal Änderungen ergeben, die auf Verbindungen zu unfreundlichen Aktueren hindeuten können.

Die Cyberagentur hat den Markt untersucht, um festzustellen, inwieweit vorhandene Technologien und kommerzielle Angebote bereits in der Lage sind, Lieferantenbeziehungen zu erfassen und zu überwachen. Dabei wurden vielversprechende, am Markt verfügbare Ansätze identifiziert, die für die Bedarfsträger der Cyberagentur relevant sind. Das daraus generierte Wissen wurde aufbereitet und weitergegeben. Zusätzlich wurden verschiedene Ansätze aus den Bereichen künstliche Intelligenz und Big Data identifiziert, die über die Grundlagenforschung hinausgehen, aber noch nicht in kommerzielle Überwachungslösungen für Lieferketten integriert wurden. Es fiel auf, dass der staatliche Blick auf Lieferketten in der Literatur bislang wenig Beachtung findet, im Gegensatz zu privatwirtschaftlichen Perspektiven.

Als zusätzliches Werkzeug kommen neue regulatorische und sozialwissenschaftliche Ansätze zur Absicherung von Lieferketten in Betracht. Daraus entstand das künftige Forschungsprojekt „Firewall für Lieferketten“ (FiLi). Die Cyberagentur wird darüber hinaus im Austausch mit den Bedarfsträgern bleiben, um Forschungsthemen zu identifizieren, die zukünftige Bedürfnisse abdecken.



ABTEILUNG SCHLÜSSELTECHNOLOGIEN

Kryptologie

Cybersicherheit durch Quantentechnologie

Cybersicherheit durch KI und Cybersicherheit für KI

Autonome Intelligente Systeme

Sichere Wege für Daten und Kommunikation

Die Forschung zu Schlüsseltechnologien wie Kryptologie, Quantentechnologie, Künstlicher Intelligenz und autonomen Systemen spielt eine entscheidende Rolle für die Weiterentwicklung der Cybersicherheit. Durch neue Verschlüsselungstechniken können Daten und Kommunikation effektiver geschützt werden, insbesondere vor den Herausforderungen durch leistungsstarke Quantencomputer. Quantentechnologien bieten auch neue Möglichkeiten für eine sichere Datenübertragung, während KI und autonome Systeme die Fähigkeit besitzen, Bedrohungen in Echtzeit zu erkennen und zu bekämpfen. Die Forschung in diesen Schlüsselbereichen trägt somit maßgeblich dazu bei, die Sicherheit von Netzwerken, Systemen und sensiblen Daten in einer zunehmend vernetzten und digitalisierten Welt zu gewährleisten.

Quantentechnologien könnten die Cybersicherheit grundlegend verändern. Einerseits könnte Quantencomputing Verschlüsselungsmethoden, die heute als sicher gelten, schnell überwinden. Dadurch würden herkömmliche Verschlüsselungstechniken wie RSA und Elliptic Curve Cryptography ihre Wirksamkeit verlieren. Auch Quantensensoren könnten in Zukunft eine wichtige Rolle in der Cybersicherheit spielen. Diese Sensoren nutzen Quanteneffekte wie die Quanteninterferenz oder die Quantenverschränkung, um extrem präzise Messungen durchzuführen. Im Referat Cybersicherheit durch Quantentechnologie wird ein mobiler Quantencomputer entwickelt, der auf die Bedürfnisse unserer Bedarfsträger ausgerichtet ist. Im Projekt „Seitenkanalangriffe mit Quantensensorik“ wird untersucht, wie sich neuartige Sensoren auf die Sicherheit von kryptografischen Systemen auswirken.

Kryptographie ist ein wichtiger Bestandteil der Cybersicherheit. Verschlüsselung sorgt dafür, dass vertrauliche Informationen sicher übertragen und gespeichert werden. Die Kryptographie entwickelt sich gerade weiter und setzt jetzt auf Verschlüsselungsalgorithmen, die gegen Angriffe durch Quantencomputer sicher sind. Zu dieser Entwicklung tragen wir mit dem Projekt „Seitenkanal-resistente Post-Quanten-Kryptologie“ bei. Außerdem entwickeln wir im Projekt „Encrypted Computing“ neue Techniken wie homomorphe Verschlüsselung und vertrauliches Rechnen. Damit können wir Daten sicher verarbeiten, ohne sie zu entschlüsseln.

Künstliche Intelligenz ist auf dem Vormarsch, auch in der Cybersicherheit. Sie ist inzwischen ein unverzichtbares Werkzeug im Kampf gegen Cyberbedrohungen. Eines der wichtigsten Einsatzgebiete von KI in der Cybersicherheit ist die Erkennung und Reaktion auf Bedrohungen. Obwohl KI zahlreiche Vorteile für die Cybersicherheit bietet, birgt sie auch neue Herausforderungen und potenzielle Bedrohungen. Ein Risiko besteht darin, dass KI-Systeme selbst Ziel von Angriffen werden könnten. Wenn Angreifer Zugriff auf KI-Algorithmen und -Modelle erlangen, könnten sie diese manipulieren, um Fehlfunktionen oder falsche Ergebnisse zu erzeugen. Dies kann zu gravierenden Sicherheitsproblemen führen, insbesondere wenn KI in sicherheitskritischen Bereichen zum Einsatz kommt.

Das Projekt „Robustes und Sicheres Machine Learning für sicherheits- und verteidigungsrelevante Einsatzsysteme“ trägt dem Umstand Rechnung, dass die zunehmende Verbreitung von KI-Technologien neue Angriffsvektoren eröffnet und die Komplexität der Cybersicherheitslandschaft erhöht. Daher ist es entscheidend, dass Organisationen proaktiv Maßnahmen ergreifen, um die Sicherheit ihrer KI-Systeme zu gewährleisten und sich gegen potenzielle Angriffe zu verteidigen. Das Projektziel ist die Erforschung und Unterstützung der Entwicklung hochresilienter, robuster und nachweisbar sicherer ML-Komponenten im hochsicherheits- und verteidigungsrelevanten Umfeld.

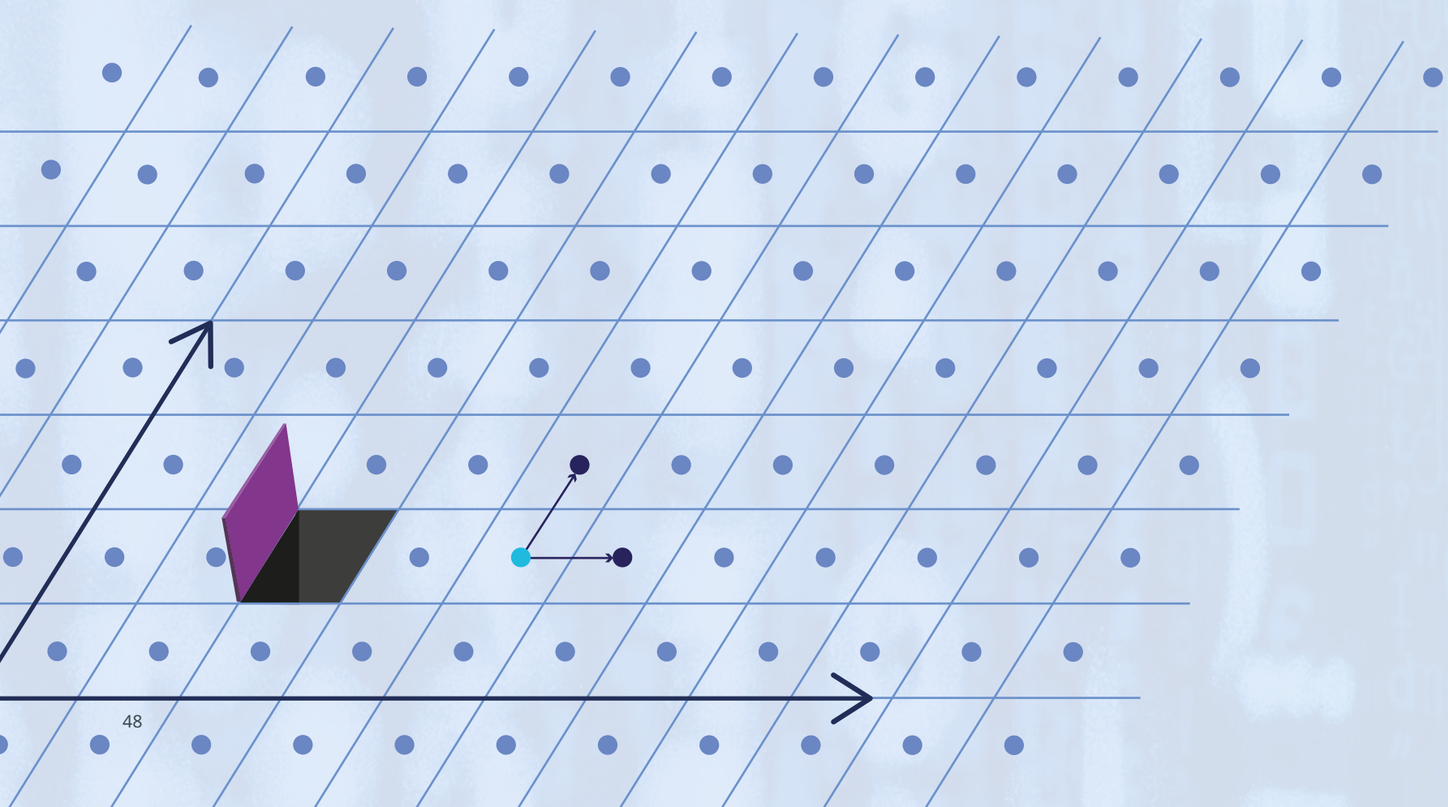
Autonome intelligente Systeme spielen eine zunehmend wichtige Rolle in der Cybersicherheit, indem sie physische Sicherheitsmaßnahmen ergänzen und erweitern. Autonome Systeme können eingesetzt werden, um in gefährlichen Umgebungen menschliche Sicherheitskräfte zu unterstützen. Das Referat Autonome Intelligente Systeme fokussiert die Forschungsaktivitäten auf Schwärme von unbemannten Systemen. So zielt das Projekt „Mobile Infrastruktur: Lageorientierung für Mobile Autonome Systeme“ darauf ab, eine mobile ad-hoc Kommunikationsinfrastruktur durch unbemannte Systeme im Verbund zu ermöglichen.

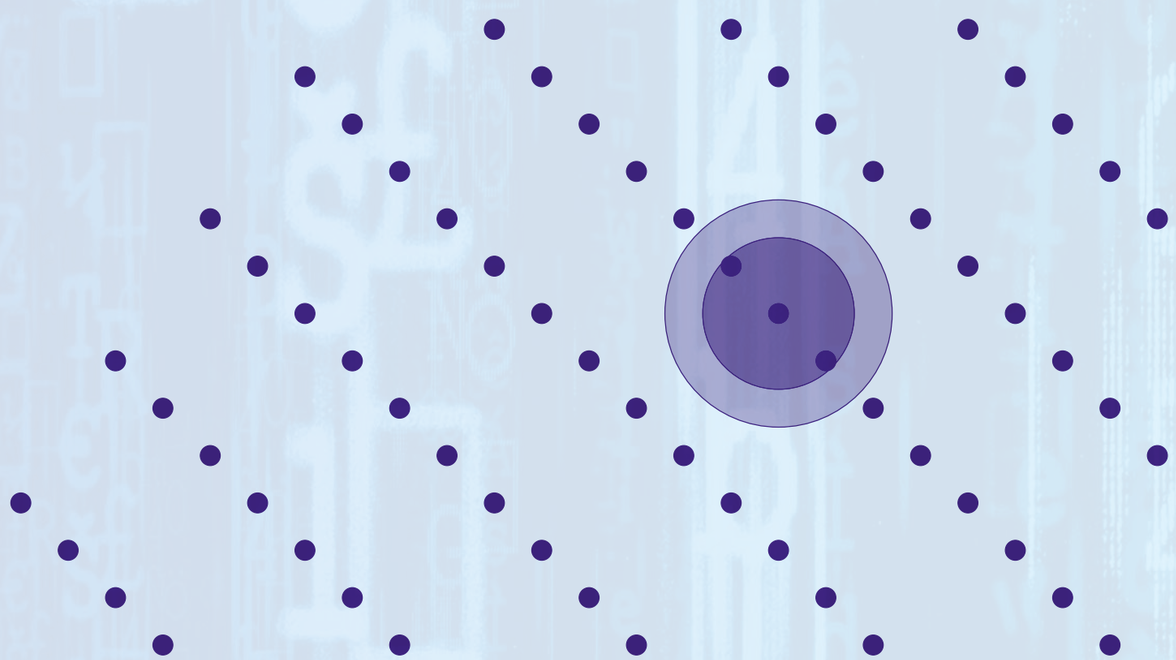
Encrypted Computing

Klassische kryptographische Verfahren schützen Daten während der Übertragung und Speicherung, ermöglichen jedoch keine Verarbeitung im verschlüsselten Zustand. Neuere Konzepte wie Encrypted Computing (EC) und Privacy-Enhancing Technology (PET) bieten hier Lösungen. Fully Homomorphic Encryption (FHE) und Multi Party Computation (MPC) erlauben es, verschlüsselte Daten zu verarbeiten, ohne diese zu entschlüsseln. Die Entschlüsselung ist nur bei Ansicht der Ergebnisse nötig, wodurch sensible Daten während der Verarbeitung geschützt bleiben. Derartige Verfahren sichern alle drei Zustände digitaler Daten und ermöglichen eine flexible Balance zwischen Datenschutz und Datennutzung.

Klassische Verschlüsselungsverfahren sind durch effiziente Algorithmen auf Quantencomputern gefährdet, da diese die zugrundeliegenden mathematischen Probleme effizient lösen können. FHE und ähnliche Verfahren basieren jedoch auf Problemen, die nach aktuellem Kenntnisstand auch für Quantenalgorithmen schwer lösbar sind und gelten daher als quantensicher und somit zukunftssicher.

Ein Anwendungsbeispiel im Bereich Cloud Computing ist Machine Learning as a Service (MLaaS). Hier kann ein Serviceanbieter Lern-Modelle auf verschlüsselten Daten auswerten, ohne die Daten selbst oder das Modell offenzulegen. Dateninhaberinnen und Dateninhaber verschlüsseln ihre Daten homomorph und senden nur diese Chiffrate an den Serviceanbieter, der sie in der verschlüsselten Domäne verarbeitet und das verschlüsselte Ergebnis zurücksendet. Die Dateninhaberin oder der Dateninhaber entschlüsselt das Ergebnis mit dem eigenen, privaten Schlüssel. Dies schützt sowohl das Modell sowie die Daten, da zu keiner Zeit die geheimen Informationen der anderen eingesehen werden können.





Encrypted Computing Compass

als Input abgeschlossener Projekte

Daten sind essenziell für ökonomische und gesellschaftliche Entscheidungen sowie wissenschaftlichen Fortschritt, müssen aber oft geschützt werden. Moderne Kryptographie ermöglicht es, mit sensiblen Daten zu rechnen, ohne deren Geheimnisse preiszugeben.

Der Encrypted Computing Compass untersucht die Praxistauglichkeit dieser Techniken, wobei drei Ansätze im Vordergrund stehen. Erstens die vollhomomorphe Verschlüsselung (FHE), ein Public Key Verfahren, das Berechnungen auf verschlüsselten Zahlen erlaubt, ohne diese zu entschlüsseln. FHE ist derzeit besonders relevant, da es bedeutende Performanzsteigerungen gab. Zweitens sind sichere Mehrparteienberechnungen (MPC) interessant, da mehrere Parteien gemeinsam Berechnungen auf geheimen Eingaben durchführen können, ohne mehr als das Ergebnis preiszugeben. MPC kann eine Alternative zu FHE mit akzeptablem Kommunikationsaufwand sein. Drittens wurden sichere Enklaven wie Trusted Execution Environments (TEEs), die durch Hardware eine abgekapselte Berechnung ermöglichen, wobei der Plattform-Betreiber keinen Zugang zu den geheimen Daten hat, als potenzielle Beschleunigung identifiziert.

Da TEEs großes Vertrauen in den Hersteller voraussetzen und daher in dem Kontext als weniger relevant angesehen werden, können sie jedoch bei geringeren Sicherheitsanforderungen eine effiziente Alternative darstellen. Eine Kombination dieser Verfahren könnte jedenfalls zukünftig vielversprechend sein, da sie unterschiedliche Sicherheits- und Effizienzniveaus vereinen kann.

Forschungsprojekt

Robustes und sicheres maschinelles Lernen (RSML)

Mehr KI-Sicherheit wagen

Künstliche Intelligenz und maschinelles Lernen (diese beiden Begriffe werden hier synonym verwendet) haben sich in den vergangenen Jahren als nützliche Werkzeuge erwiesen. Sei es beim autonomen Fahren, als Chatbots oder in der Cybersicherheit: KI hat sich dank steigender Performance und zunehmender Vielseitigkeit zu einem Werkzeug zur Erzeugung und Analyse immer größerer und komplexerer Datenmodelle entwickelt. Angesichts des hohen Entwicklungstempos und der offenen Grenzen des Machbaren lag der Fokus bei der Entwicklung von KI bislang auf der Leistungsmaximierung und Modelloptimierung mit Blick auf die angestrebten Funktionalitäten; ein Chatbot sollte sich zum Beispiel zu möglichst vielen Themen versiert äußern, eine Objekterkennung möglichst viele Testobjekte exakt klassifizieren. Andere Qualitätsmerkmale wie beweisbare Sicherheit und inhärente Robustheit in unvorhergesehenen Situationen oder bei gezielten Angriffen wurden oft hintenangestellt.

Dies ist bemerkenswert, denn aus Perspektive der IT-Sicherheit sind Systeme mit KI genauso schützenswert wie andere Systeme: Sie sind potenziell den gleichen Bedrohungen und Angriffen ausgesetzt, können im Fall einer Fehlfunktion eine ähnliche große Bedrohung für Mensch und Umwelt darstellen und sie schützen unter Umständen ebenso schützenswerte Daten. KI als Softwarekomponente ist einer ähnlich problematischen Sicherheitslage ausgesetzt, wie andere Systeme; dies zeigen unter anderem jüngere Meldungen über neu gefundene KI-Sicherheitslücken, zum Beispiel bei Chatbots oder beim autonomen Fahren.

Neue Angriffsmöglichkeiten gegen KI

Zugespitzt wird diese Lage durch das Aufkommen neuartiger Angriffsvektoren, die gezielt Eigenschaften von KI ausnutzen. Die Grundlage hierfür: KI verfolgt einen datengetriebenen Ansatz und wichtige Funktionalitäten werden nicht explizit programmiert, sondern anhand von Beispielen trainiert. Folglich haben unbewusste Verzerrungen oder absichtliche Manipulationen in den Trainingsdaten direkte Auswirkungen auf das gelernte Programm – Angreifer können so analog zu klassischer Software ihren eigenen Code in die Ausführung der KI „einschleusen“. Wenn ein KI-System zusätzlich noch dazu ausgelegt ist, sich aufgrund von Umwelteinflüssen ständig zu verändern oder das Training auf mehreren Rechnern verteilt stattfindet, kann die Qualitätssicherung zu einem schwer kontrollierbaren Problem werden. Dieses Beispiel zeigt neben vielen anderen: Ungesicherte KI kann zu einem ernsten Problem für die IT-Sicherheit werden.

KI-Absicherung mit mehreren Schwerpunkten

Hier setzt das Projekt RSML an. Im Mittelpunkt des Vorhabens steht die Erforschung, Entwicklung und Anwendung neuartiger Ansätze zur Steigerung der Robustheit und Sicherheit von KI-Systemen im Kontext von Einsatzsystemen in den Domänen der Inneren und Äußeren Sicherheit. Bei den Forschungs- und Entwicklungstätigkeiten sollen sowohl konzeptionelle als auch modell- bzw. anwendungsbezogene Fragen adressiert werden. Ziele des Projekts sind wissenschaftlicher und technologischer Fortschritt, um inhärente Sicherheitseigenschaften von KI-Komponenten zu verbessern, sowie die Umsetzung dieser Ansätze im Rahmen von Demonstratoren oder Prototypen. Darüber hinaus sollen innovationstreibende Netzwerke gebildet werden. Das Miteinander von Bedarfsträgern, Industrievertretern und Forschenden wird zur Stärkung der digitalen Souveränität Deutschlands beitragen.

Um innovative Ansätze entlang von fünf Forschungsschwerpunkten des Projekts für ein breites Spektrum an möglichen Zukunftsanwendungen zu realisieren, beauftragt die Cyberagentur mehrere Bieterinnen oder Bietergemeinschaften parallel. Im Rahmen eines „Wettbewerbs der Ideen“ werden die Ergebnisse phasenweise evaluiert und das Teilnehmerfeld schrittweise verkleinert. Der überzeugendste Ansatz verbleibt bis zum Abschluss der letzten Phase im Wettbewerb. Die Evaluation geschieht mithilfe einer Jury, die aus Mitgliedern der Cyberagentur, des Bundesamts für Sicherheit in der Informationstechnik und dem Kommando Cyber- und Informationsraum der Bundeswehr besteht. In der letzten Phase des Wettbewerbs erhält eine ausgewählte Teilnehmerin oder ein ausgewählter Teilnehmer die Möglichkeit, entwickelte Software-Artefakte im Rahmen einer realistischen Testumgebung zu erproben.

Forschungsprojekt

Seitenkanalangriffe mit Quantensensorik (SCA-QS)

Viele sicherheitsrelevante Aktivitäten im Alltag beruhen auf der Verschlüsselung mit elektronischen Chips. Daher beschäftigt sich ein ganzes Forschungsfeld mit sogenannten Seitenkanalangriffen (SCA, side-channel attacks), um deren Verschlüsselungen einerseits zu umgehen, andererseits dagegen zu härten. Für diese Angriffe können verschiedene Arten von Sensoren verwendet werden, die Informationen über die Daten auf dem Chip erfassen. Diese Informationen werden analysiert, um Schlüssel, Passwörter oder andere sensible Daten zu ermitteln.

Die Entwicklung verbesserter Sensoren und die Entdeckung neuer Schwachstellen in Mikrochips kann als ein Zyklus kontinuierlicher Verbesserungen betrachtet werden, bei dem Fortschritte in der Messtechnik zur Entdeckung neuer Schwachstellen führen, die wiederum die Entwicklung besserer Sicherheitsmaßnahmen vorantreiben. Da in absehbarer Zukunft eine Reihe neuer Quantensensoren (QS) auf den Sensormarkt drängt, besteht die Gefahr, dass dieser Kreislauf auf beiden Seiten unterbrochen wird. Dadurch erhielten Seitenkanalangriffe einen erheblichen Vorteil und die etablierten Sicherheitssysteme könnten verwundbar werden.

Das Forschungsprojekt SCA-QS zielt daher darauf ab, die Anwendung von Quantensensoren zur Identifikation neuer Angriffsvektoren auf Mikrochips zu erforschen. Es konzentriert sich dabei zunächst auf die Identifikation und Erforschung der grundsätzlichen Eignung von Quantensensorik für Seitenkanalangriffe, um im Anschluss ggf. erfolgversprechende Ansätze weiterzuentwickeln.

Die Ausschreibung des Projekts erfolgte im Juni 2024.

Forschungsprojekt

Mobile Infrastruktur – Lagewahrnehmung für Mobile Autonome Systeme (MoIn-LaMAS)

Autonome Systeme wie Drohnen und Bodenfahrzeuge werden in Zukunft eine größere Bedeutung für die Gewährleistung der öffentlichen Sicherheit haben. Die Leistungsfähigkeit dieser Systeme wird durch den Einsatz im homogenen oder heterogenen Verbund bzw. Schwarm weiter erhöht. Das Projekt MoIn-LaMAS zielt darauf ab, zukünftig eine mobile Ad-hoc-Kommunikationsinfrastruktur zu ermöglichen, indem unbemannte Systeme im Verbund lageabhängig verlegbare Relais in einem Gebiet platzieren.

Kommunikationsnetzwerke stellen für jegliche Anwendungsbereiche der Inneren und Äußeren Sicherheit das Rückgrat der Koordinierung von Personen, Verbänden und Logistik dar. Entsprechend wichtig ist eine ununterbrochene Kommunikation mit und zwischen Einsatzteilnehmerinnen und -teilnehmern. In Gebieten mit natürlichen oder dynamischen Störquellen, ist die Aufrechterhaltung effektiver Kommunikation dabei besonders herausfordernd. Die verstärkte Nutzung von modernen Methoden der elektronischen Kriegsführung sowie unkontrollierbare Umgebungsbedingungen stellen zusätzlich eine große Herausforderung dar.

Die besondere Stärke von MoIn-LaMAS liegt in der autonomen dynamischen Rekonfigurierbarkeit, die aktiv auf Auftrags-, Umgebungs- oder Lageänderungen reagiert. Um diese Autonomie und Dynamik zu gewährleisten, werden neuartige Methoden zur Erzeugung eines multifaktoriellen Lagebildes für Einsatzszenarien entwickelt, in denen Kommunikations- und Navigationsdienste großflächig nicht verfügbar sind.

Die Ausschreibung des Projekts wird für Q4/2024 angestrebt.

Forschungsprojekt

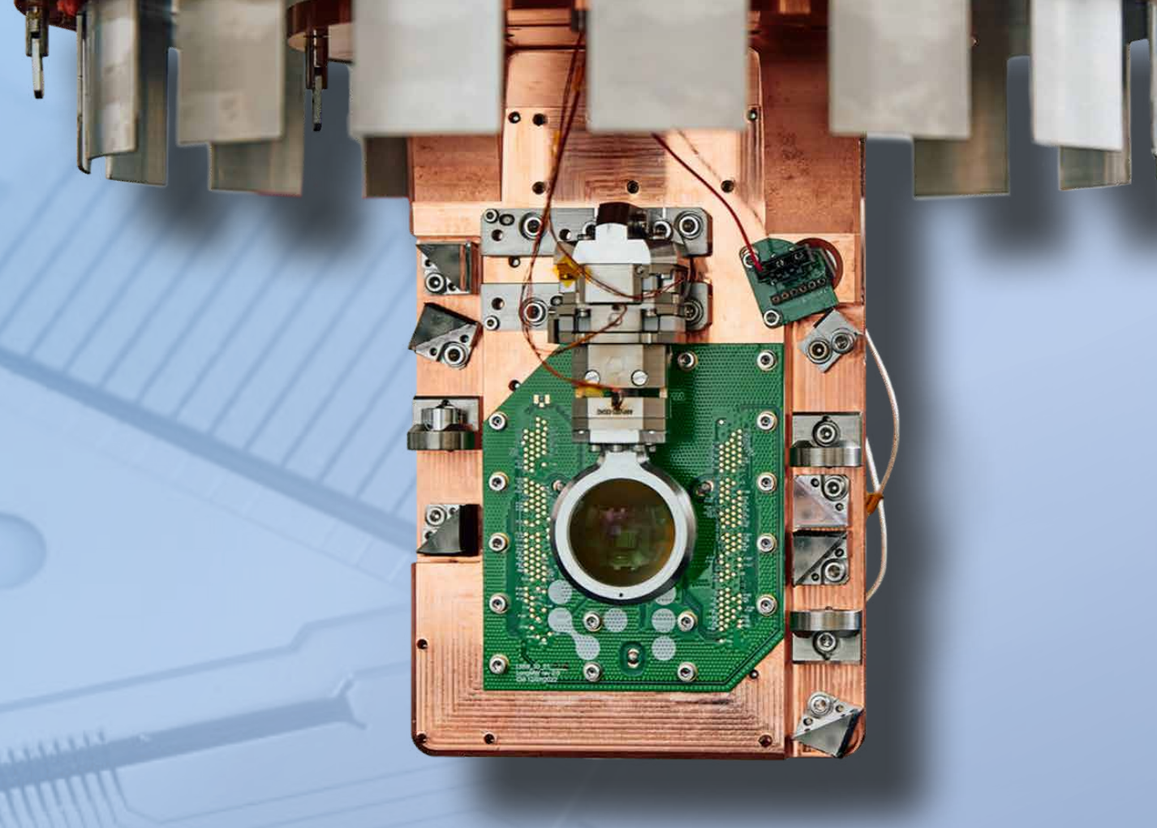
Mobiler Quantencomputer (MQC)

Es ist zu erwarten, dass Quantencomputer in absehbarer Zeit das Computing revolutionieren werden, da diese eine massive Parallelisierung bestimmter Rechenvorgänge erlauben, die für klassische Computer unmöglich sind. Daraus kann sich ein erheblicher Geschwindigkeitsvorteil für konkrete Anwendungen ergeben, z.B. für Optimierungsprobleme, großskalige Simulationen, im Zusammenhang mit der Analyse großer Datenmengen und der Kryptographie. Bislang haben Faktoren wie die Miniaturisierung des Gesamtsystems inklusive der Peripheriegeräte, der Energieverbrauch oder das Gewicht der Systeme bei der Forschung kaum eine Rolle gespielt. Mobile Systeme sind insbesondere für den Einsatz in Sicherheits- und Verteidigungsszenarien von großem Interesse, da sie nicht auf eine Datenanbindung an ein stationäres Rechenzentrum mit Quantencomputern angewiesen sind. Insbesondere im Krisen- oder Verteidigungsfall ist die jederzeitige Verlegbarkeit wichtig. Aber auch für zahlreiche andere Anwendungen im In- und Ausland bieten kleine, mobile Systeme unschätzbare Vorteile.

Das Forschungsprojekt „Mobiler Quantencomputer – Quantenprozessoren für den mobilen Einsatz in Verteidigungs- und Sicherheitsanwendungen“ verfolgt das Ziel, im Bereich der Quantencomputerforschung mit Blick auf Anwendungsszenarien in den Bereichen Sicherheit und Verteidigung die Aspekte Ortsunabhängigkeit, Mobilität bzw. schnelle Verlegbarkeit unter Berücksichtigung der dafür relevanten Parameter wie z.B. Größe, Gewicht oder Energieverbrauch frühzeitig mitzudenken und zu erforschen. Zugleich soll die Steigerung der Leistungsfähigkeit gegenüber aktuellen Quantenprozessoren signifikant vorangetrieben werden.

Das Hauptziel des Projekts besteht darin, zum Ende der Projektlaufzeit den Laboraufbau eines vollständig mobilen Quantencomputers zu erhalten, an dem Tests durchgeführt werden können, für welchen erste Versuchsanwendungen geschrieben und erprobt werden können und auf Basis dessen in Zukunft die Entwicklung leistungsfähiger mobiler Systeme durchgeführt werden kann. Darüber hinaus ist das Ziel die Miniaturisierung aller Komponenten eines Quantencomputers, inklusive der zur Steuerung notwendigen Peripheriegeräte.

Aus technischer Perspektive ist das Ziel der Aufbau und Funktionsnachweis eines reproduzierbaren und programmierbaren Quantenprozessors, der mobil, kompakt, leicht, energieeffizient und robust gegenüber sich ändernden Umgebungsbedingungen ist. Dabei soll die Leistung des Quantenprozessors zugleich möglichst groß ausfallen.
Für die physische Realisierung der Qubits eines Quantenprozessors gibt es dabei eine Reihe verschiedener Forschungsansätze, die alle Vor- und Nachteile aufweisen. Obgleich die Ansätze sehr unterschiedlich weit fortgeschritten sind, ist bislang nicht absehbar, welche davon sich durchsetzen werden. Mehrere Ansätze haben das Potenzial, sich für mobile Anwendungen einsetzen zu lassen. Insofern soll sich im Verlauf des Projektes auch zeigen, inwieweit sich die verschiedenen Systeme tatsächlich für leistungsfähige, mobile Quantencomputer eignen.



Mitte Dezember 2022 erfolgte die Ausschreibung des Projektes im Rahmen eines PCP-Verfahrens. Aus den Bewerbungen wurden 15 Interessentinnen und Interessenten ausgewählt, die in die erste von vier Phasen des Wettbewerbs starteten. Die Wettbewerberinnen und Wettbewerber setzten sich dabei aus insgesamt 49 potenziellen Haupt- und Unterauftragnehmern zusammen, sieben davon akademische Einrichtungen, die anderen aus der Industrie, darunter zahlreiche Startups. Unter den Anträgen befanden sich zudem neun Teilnehmerinnen und Teilnehmer aus dem Ausland.

Eine Expertenjury aus Projektmitarbeitern und -mitarbeiterinnen der Cyberagentur sowie externen Fachleuten evaluierte die eingegangenen Kurzkonzepte. Die sechs bestbewerteten Bieterinnen und Bieter kamen weiter in die Phase 2 des Wettbewerbs und erarbeiteten daraufhin bis August 2023 Detailkonzepte mit einem Umfang von je bis zu 100 Seiten. Auch diese wurden von der Expertenjury evaluiert. Mit den drei am besten bewerteten Angeboten, die dem hohen, innovativen Ansatz entsprachen, wurde in ausführliche Verhandlungen eingetreten. Anschließend konnte der Start in die Hauptforschungsphase – Phase 3 – Ende Juli 2024 vollzogen werden.

Fotos: Oxford Ionics (oxionics.com) - neQxt (neqxt.org)

IDEENWETTBEWERB DER CYBERAGENTUR

HAL2025

HAL2025 **Auf der Suche nach den Ideen von übermorgen**

Der Einsatz von unbemannten autonomen Systemen nimmt durch die wachsenden technischen Möglichkeiten im Bereich Robotik, Sensorik und Künstliche Intelligenz weltweit zu. Es ist anzunehmen, dass solche autonomen Systeme, wie z.B. Drohnen für die Aufklärung in Krisen- oder Katastrophenfällen oder unbemannten Bodenfahrzeugen zur Unterstützung von Logistik und Transport in Konfliktfällen, zukünftig vermehrt in Schwärmen eingesetzt werden – bis hin zu autonom durch künstliche Intelligenz selbst- oder fremdgesteuerten emergenten Verbünden.

Viele technische Entwicklungen sind in diesen Bereichen aufgrund der Neuartigkeit der eingesetzten Technologien noch am Anfang ihrer Möglichkeiten. Es ist jedoch davon auszugehen, dass die Innovationen im Bereich der Autonomen Systeme in den kommenden zehn bis 15 Jahren stetig voranschreiten und mit einer entsprechenden Befähigung sowohl im militärischen als auch im zivilen Bereich einhergehen wird – sowohl bei den deutschen Bündnispartnern als auch bei Ländern, die nicht im Sinne der deutschen Sicherheitsinteressen handeln.

Deshalb sucht der bundesweite Ideenwettbewerb HAL2025 nach innovativen Konzepten im Bereich „Autonome Intelligente Systeme im Schwarm“, die eine hohe Relevanz für die Innere und Äußere Sicherheit Deutschlands haben. Durch die öffentlichkeitswirksame Ausschreibung des Ideenwettbewerbes versucht die Cyberagentur, einen möglichst breiten Adressatenkreis zu erreichen, um eine große Vielfalt an Ideen und Lösungsansätzen zu generieren. Die beste eingereichte Idee wird mit einem Preisgeld von 100.000 Euro prämiert und dient anschließend als Grundlage für eine Projektausschreibung der Cyberagentur im Bereich Autonomer Intelligenter Systeme im Schwarm.

Das Projekt wird durch das Bundesministerium der Verteidigung und das Bundesministerium des Innern und für Heimat unterstützt.

Ein starkes Netzwerk

Von der innovativen Idee bis zur Ausschreibung – Prozesse mit vielen Bearbeitungs- und Prüfungsstufen kennzeichnen die Arbeit an den Forschungsfragen der Cyberagentur. Das kann schon bis zu einem Jahr dauern. Durch Transparenz und Aufklärung schafft die Cyberagentur Verständnis, welchen zeitlichen Aufwand dies bedeutet. Es geht schließlich um Gelder für bahnbrechende und hochrisikobehaftete Grundlagenforschung auf dem Gebiet der Cybersicherheit.

Besuche in Halle an der Saale, in Berlin, in Dresden, München, Köln. Wo immer Parlamentarierinnen und Parlamentarier, Forschende, Startups oder Unternehmen wissen wollten, woran die Cyberagentur arbeitet, wurde Aufklärungsarbeit betrieben. Formate wurden entwickelt, um Forschungsprojekte und Hintergründe des wissenschaftlichen Tuns näher zu bringen.

Auf dem Security and Innovation in Cyberspace – SIC!, dem ersten wissenschaftlichen Fachsymposium der Cyberagentur, trafen sich im Juni 2023 rund 200 Expertinnen und Experten in der HÄNDEL HALLE in Halle (Saale) zum inhaltlichen Austausch zu bahnbrechenden Forschungsthemen sowie zum Netzwerk- und Communitybuilding mit Teilnehmenden aus dem Bereich der Cybersicherheit von Wissenschaft und Forschung, Industrie und Startups, Behörden, Bundeswehr und Ministerien.

der Souveränität von übermorgen

Im September 2023 wurde offen mit Mitgliedern des Deutschen Bundestages diskutiert.
Der 1. Parlamentarische Abend der Cyberagentur in der Deutschen Parlamentarischen Gesellschaft.
Den Parlamentarierinnen und Parlamentariern wurde ein informativer Überblick über die Aufgaben, Ziele und Projekte der Cyberagentur verschafft. Von den Teilnehmenden sowie den Rednerinnen und Rednern des Abends wurde ausdrücklich die spannende Diskussionsrunde des Abends und der offene Austausch unter den Diskussionsteilnehmenden gelobt.

Ebenfalls im September richtete die Cyberagentur die internationale Jahrestagung der Kriminologen „Annual Human Factor in Cybercrime Conference" in Halle (Saale) aus.

Zu vielen Fachkonferenzen im In- und Ausland wurden die Wissenschaftlerinnen und Wissenschaftler der Cyberagentur eingeladen, um die Projekte und zukunftsweisenden Ideen zu präsentieren. Vorträge, Workshops, Informationsstände und Talkrunden. Wo immer über digitale Forensik, Künstliche Intelligenz, Cyberkriminalität oder Mensch-Maschine-Interaktion diskutiert wurde, brachte sich die Cyberagentur ein.

Getrieben sind wir durch die Nationale Sicherheitsstrategie, die uns den Auftrag des Ausbaus mitgegeben hat. Auftrag, Herausforderung und Chance, die Souveränität von übermorgen zu gestalten.

für die Cybersicherheitsforschung

cyberagentur

Impressum

Agentur für Innovation in der Cybersicherheit GmbH
Große Steinstraße 19
06108 Halle (Saale)

Geschäftsführer: Prof. Dr. Christian Hummert, Daniel Mayer
Vorsitzender des Aufsichtsrats: Dr. Christian Mrugalla

Kontakt für Medien und andere redaktionelle Anfragen:
E-Mail: presse@cyberagentur.de

Idee / Redaktion / Layout: Cyberagentur
Druck: Impress Druckerei Halbritter KG · Halle (Saale)

Redaktionsschluss: 31. August 2024

www.cyberagentur.de