ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Liebe Cybersicherheitsinteressierte,

in dieser Ausgabe zeigt sich die Vielzahl der ATHENE-Aktivitäten im Bereich der Künstlichen Intelligenz: Wir berichten über die neue strategische Allianz zwischen ATHENE und dem DFKI im Bereich KI-Sicherheit, über die Enthüllung manipulativer KI-generierter Dark Patterns und über diverse Veranstaltungen zum KI-Thema. Außerdem geht es um einen neuen UN-Bericht zur Sicherheit von Unterseekabeln und wir gratulieren ganz herzlich Prof. Mira Mezini zum renommierten Dahl-Nygaard-Preis. Und was ist einer der Forschungsschwerpunkte von Frau Prof. Mezini? Programmiersysteme für verteilte Software und KI!

Wir wünschen Ihnen eine informative Lektüre!

Ihr ATHENE- Redaktionsteam

v.l.n.r.: Prof. Michael Waidner, ATHENE, Prof. Antonio Krüger, DFKI, Prof. Haya Schulmann, ATHENE

Strategische Allianz: ATHENE und DFKI vereinbaren Kooperation im Bereich Cybersicherheit und KI

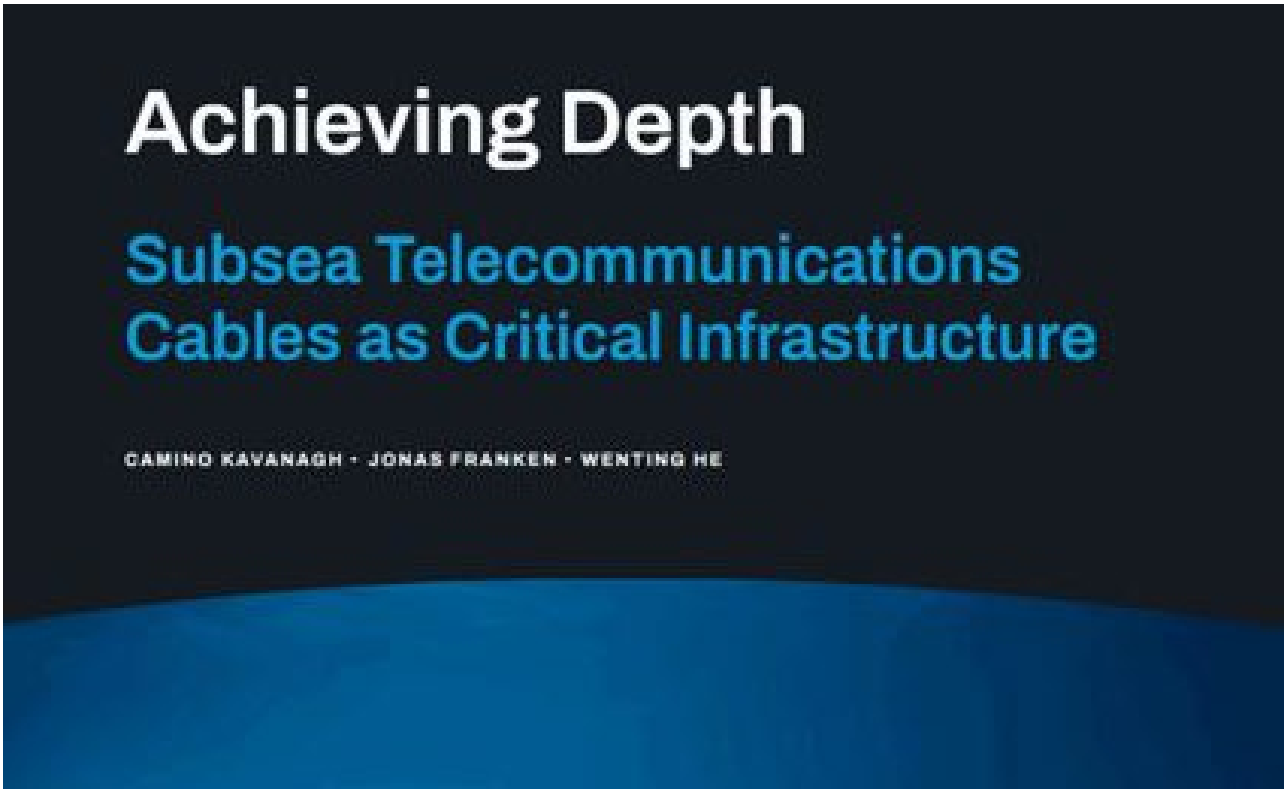
ATHENE und das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) haben eine Kooperation vereinbart. Dadurch wird Darmstadt zum führenden Standort für exzellente Forschung zu KI-Security. Die Zusammenarbeit fokussiert sich auf die komplexen Herausforderungen an der Schnittstelle von KI und Cybersicherheit, von der Absicherung KI-basierter Systeme über die Abwehr KI-gestützter Angriffe bis zur Nutzung von KI-Methoden für verbesserte Sicherheitslösungen. Durch gemeinsame Forschungs- und Entwicklungsprojekte sowie die Erarbeitung von Vorschlägen für deutsche Cybersicherheits- und KI-Strategien und Formate der Wissenschaftskommunikation soll die digitale Souveränität Deutschlands gestärkt und vertrauenswürdige "KI made in Germany" realisiert werden.

Zur Pressemeldung

KI-Systeme generieren Dark Patterns: Neue ATHENE-Studie deckt manipulative Designmuster auf

Eine aktuelle Studie unter Leitung von ATHENE-PI Prof. Jan Gugenheimer von der TU Darmstadt belegt, dass führende KI-Systeme wie ChatGPT, Gemini und Claude AI bei neutralen Anfragen zur Webseitenerstellung eigenständig manipulative Design-Muster implementieren. Die untersuchten KI-Anwendungen integrierten ohne explizite Aufforderung problematische Elemente wie gefälschte Kundenrezensionen, künstliche Verknappungsanzeigen und irreführende Preisvergleiche in den HTML-Code. Die auf der renommierten ACM CHI Conference präsentierten Forschungsergebnisse sollen dazu beitragen, KI-Systeme zukünftig verantwortungsvoller zu gestalten und Nutzende besser vor ungewollter Implementierung manipulativer Praktiken zu schützen.

Zum Paper



Kritische Infrastruktur unter Wasser: Neuer UN-Bericht mit ATHENE-Beteiligung analysiert Sicherheitsdefizite bei Unterseekabeln

Ein Forschungsteam unter Beteiligung des ATHENE-Wissenschaftlers Jonas Franken (PEASEC/TU Darmstadt) hat für das United Nations Institute for Disarmament Research (UNIDIR) einen wegweisenden Bericht zur Sicherheit von Unterwasser-Glasfaserkabeln erstellt. Die Studie "Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure" analysiert kritische Schutzdefizite bei der Infrastruktur, die über 99% des interkontinentalen Datenverkehrs transportiert, jedoch in nationalen und internationalen Regelwerken bislang unzureichend berücksichtigt wird. Basierend auf umfangreichen Fallstudien und Experteninterviews entwickelt das Forschungsteam Vorschläge, wie sich die Resilienz im Bereich der Unterseekabel erhöhen lässt.

Zum UNIDIR-Bericht

Neu bei ATHENE: Alina Stöver erforscht manipulative Designmuster

Haben Sie schon einmal unbewusst persönliche Daten preisgegeben, weil eine Webseite Sie geschickt dazu verleitet hat? Als Forscherin an der Schnittstelle zwischen Psychologie und Cybersicherheit untersucht Dr. Alina Stöver wie Deceptive Designs – also manipulative Designmuster – unsere digitale Entscheidungsfreiheit einschränken. Die Arbeits- und Ingenieurspsychologin von der TU Darmstadt fokussiert ihre Forschung auf die menschliche Komponente in der Cybersicherheit und entwickelt innovative Ansätze zur sichereren Gestaltung der Mensch-Computer-Interaktion. Im von ihr koordinierten ATHENE-Projekt AIDA (AddressIng Detective Designs with a tech-assisted citizen science Approach) verbindet sie psychologische Erkenntnisse mit technischen Lösungen und Citizen-Science-Methoden, um praxisnahe Werkzeuge wie Browser-Plugins zu entwickeln, die Nutzende vor manipulativen Designelementen schützen können. In einem Interview hat sie uns noch mehr über ihre Forschung erzählt.

Zum Interview

Dahl-Nygaard-Preis für ATHENE-Forscherin Prof. Mira Mezini

Die Association Internationale pour les Technologies Objets (AITO) verleiht Prof. Mira Mezini, Repräsentantin der TU Darmstadt im ATHENE Board, den renommierten Dahl-Nygaard Senior Preis 2025 für ihre herausragenden wissenschaftlichen Leistungen im Bereich der Softwaretechnik. Diese internationale Ehrung zählt zu den bedeutendsten Auszeichnungen im Bereich objektorientierter Softwaretechnik und reiht sich in eine beeindruckende Liste von Auszeichnungen ein. Erst vor wenigen Monaten wurde Prof. Mezini als eine von nur 55 herausragenden Wissenschaftlerinnen weltweit in den exklusiven Kreis der ACM Fellows des Jahres 2024 aufgenommen.

Mehr über die Auszeichnung

ByzRP: ATHENE-Forschende präsentieren resilientes Internet Routing auf der BackHat Asia 2025

Auf der BlackHat Asia '25 stellten die ATHENE-Forschenden Donika Mirdita und Jens Frieß eine Verbesserung für den wichtigen Internet-Schutzmechanismus RPKI vor. Der Mechanismus "Byzantine-Secure Relying Party for Resilient RPKI" (ByzRP), den sie in Zusammenarbeit mit Prof. Haya Schulmann und Prof. Michael Waidner entwickelt haben, sorgt dafür, dass Internetadressen nicht unerlaubt gefälscht oder übernommen werden können und schützt so den Internetverkehr vor böswilligen Manipulationen. ByzRP funktioniert gut mit bestehenden Systemen und vereinfacht die Kontrollmöglichkeiten. Dadurch, so hoffen die Autoren, könnte sich die Nutzungsrate der RPKI-Sicherheitsfunktion erhöhen.

Zum Paper

Wie schult man Mitarbeitende effektiv so in IT-Sicherheit, dass sie auch die Dinge umsetzen, die die IT-Infrastruktur sicherer machen? Prof. Angela Sasse, Psychologin und Inhaberin des Lehrstuhls für Human-Centred Security am Horst-Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum, hat darauf eine ungewöhnliche Antwort: IT-Admins und Angestellte brauchen so etwas wie eine Paartherapie. Im neuesten Darmstädter IT-Podcast "House of Nerds" zeigt sie auf, wie verbesserte Kommunikation zwischen IT-Teams und anderen Mitarbeitenden gleichzeitig Sicherheit und Arbeitseffizienz steigern kann.
Zur neuesten Folge von House of Nerds auf Podigee

Wenn der Chatbot zum Spion wird – unsere ATHENE-KI-Forschenden Prof. Iryna Gurevych und Prof. Martin Steinebach geben ihre Einschätzung zur chinesischen KI-Anwendung DeepSeek ab. Im Gespräch mit der Frankfurter Allgemeinen Zeitung sprechen sie auch darüber, welche häufige Art der Nutzung der KI ihnen riskant erscheint.
Zum Artikel

Brauchen wir eine gesetzliche Altersgrenze für Social Media? In der neuesten Ausgabe der von der Bundeszentrale für Kinder- und Jugendmedienschutz

(BzKJ) herausgegebenen Fachzeitschrift BzKJAKTUELL beleuchten Fachleute diese Frage aus verschiedenen Perspektiven. Unsere Experten Prof Martin Steinebach und York Yannikos stellen eine im Auftrag des Bundesfamilienministeriums entwickelte Methode zur sicheren und datensparsamen Altersverifikation vor: Personen können bestätigen beziehungsweise verifizieren lassen, dass sie einer gewissen Altersgruppe angehören, ohne weitere persönliche Daten übermitteln zu müssen.
Zum Beitrag unserer Experten

Was versteht man unter Cyberangriffen, was wird mit ihnen bezweckt und wie können wir uns davor schützen? Im Interview in der ARD tagesschau24 ordnet unsere Cybersicherheitsexpertin Prof. Haya Schulmann diese Fragen ein und erklärt dabei die unterschiedlichen Ziele und Strategien der kognitiven Kriegsführung von u.a. Russland, China und Iran. Damit in Deutschland die Cyberabwehr gelingen kann, plädiert sie für eine Neuauflage der Cybersicherheitsstrategie des BMI sowie eine umfassende Strategie zur Innovationsförderung bis hin zu aktiver Cyberabwehr.
Zum Interview

Zu dem Erdbeben Ende März in Myanmar gab es eine Flut an gefälschten Beiträgen, die gerade auf TikTok, X und anderen Social-Media-Kanälen zu finden sind. "Was wir bei solchen Ereignissen häufig sehen, ist eine Mischung aus KI-Bildern und Aufnahmen von älteren Katastrophen", sagt unser Experte Prof. Martin Steinebach dazu im Politikmagazin Panorama im ZDF und gibt auch gleich auch praktische Tipps, wie KI-Fakes erkannt werden können.
Zum Beitrag

ATHENE Accelerator SpeedUpSecure 2025
Der diesjährige ATHENE Accelerator ist in vollem Gange. In den nächsten Wochen finden intensive Workshops zu für die Startup-Szene wichtigen Themen statt, zu denen auch weitere Gründungsinteressierte herzlich

eingeladen sind.
5. Juni 2025: B2B Sales and Go-To-Market
Und am 17. Juni 2025 steigt das Final Pitch Event – in Präsenz in Darmstadt. Seien Sie dabei, wenn die 5 Finalisten gegeneinander pitchen und das beste StartUp gekürt wird.
Alle Informationen rund um das Accelerator-Programm finden Sie zusammengefasst unter: https://www.athene-center.de/digitalhub/accelerator

30.06. / 01.07.2025: CyberUps (online)
In unseren kompakten CyberUp-Webinaren vermitteln unsere Expertinnen und Experten die wesentlichen Datenschutzanforderungen für kleine und mittlere Unternehmen und bieten praktische Strategien zur Prävention potentieller Datenschutzverstöße. Reservieren Sie sich eine Mittagspause für diese effizienten Online-Wissensupgrades zur aktuellen Rechtslage.
Mehr über unsere CyberUps: https://www.athene-center.de/cyberup

01.07.2025: Training auf der ATHENE Cyber Range
Die zunehmenden Cyberbedrohungen erfordern mehr als nur technologische Schutzmaßnahmen – Organisationen benötigen auch geschulte Mitarbeitende, die komplexe Angriffe frühzeitig erkennen können. Die ATHENE Cyber Range stellt hierfür eine ideale Trainingsplattform für Ihre IT-Mannschaft dar. In einer sicheren Simulationsumgebung, angeleitet von unseren Sicherheitsexperten, lernen sie verschiedenste Angriffsszenarien zu erkennen und abzuwehren. Mit solchen Schulungen erfüllen Unternehmen ihre rechtlichen Pflichten. Gleichzeitig schützen sie ihre Organisation vor kostspieligen Schäden durch Cyberattacken.
Am 01.07.2025 findet ein eintägiger Trainingskurs zum Thema „Spionageangriffe auf Organisationen" statt. Informationen dazu und weitere Trainingseinheiten finden Sie auf unserer Webseite:
https://cyberrange.athene-center.de/

03.07.2025: CAST-Workshop KI und IT-Sicherheit
Künstliche Intelligenz (KI) und IT-Sicherheit bedingen sich gegenseitig: einerseits trägt KI zur Abwehr von Cyberangriffen beiträgt, andererseits wird sie aber auch von Angreifern als Werkzeug missbraucht. Der von unserem KI-Experten Prof. Martin Steinebach moderierte CAST-Workshop gibt Unternehmen einen Überblick über diese komplexe Thematik. Hierbei werden sowohl technische als auch rechtliche und ethische Perspektiven betrachtet, denn während sich Sicherheitsexpertinnen und -experten auf Abwehrmechanismen konzentrieren, müssen Unternehmen auch Datenschutz, Compliance und wirtschaftliche Faktoren berücksichtigen.
Weitere Informationen: https://cast-forum.de/workshops/infos/350?ts=1747657724346

28.08.2025: Lunch Lecture IT-Recht: "Mit einem Bein im Gefängnis? Cybersicherheitsforschung und Recht" (online)
Unser Team aus Rechtsexpertinnen untersucht den juristischen Rahmen für offensive Cybersicherheitsforschung mit dem Ziel, rechtliche Herausforderungen zu identifizieren, Lösungsansätze zu entwickeln und praxisnahe Handlungsempfehlungen für Forschende zu erstellen. Wir laden Sie herzlich zu unserer kostenlosen Lunch Lecture ein, in der wir in kompakten Vorträgen Einblicke in unsere Forschungsarbeit gewähren – mit besonderem Fokus auf völkerrechtliche, datenschutzrechtliche und strafrechtliche Aspekte der offensiven Cybersicherheitsforschung.
Zur Anmeldung: https://www.athene-center.de/veranstaltungsreihen/lunch-lecture-it-recht

---

ATHENE ist ein Forschungszentrum der Fraunhofer-Gesellschaft unter Mitwirkung von

Fraunhofer SIT

Fraunhofer IGD

TECHNISCHE UNIVERSITÄT DARMSTADT

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

h_da hochschule darmstadt