ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Liebe Cybersicherheitsinteressierte,

in den vergangenen Wochen ist viel passiert bei ATHENE, neben Forschungserfolgen auf internationalen Konferenzen ging es um Politik und internationale Zusammenarbeit: Vor zahlreichen Hochschulvertreterinnen und -vertretern stellte Prof. Dr. Haya Schulmann vergangene Woche die Ergebnisse der Langzeitstudie zur Cybersicherheit der deutschen Universitäten vor und leistete damit einen wichtigen Beitrag zum nationalen Lagebild der Bundesrepublik. Über Deutschland hinaus stärkt ATHENE die transatlantische Cybersicherheitsforschung durch ein Memorandum of Understanding zwischen der Goethe-Universität Frankfurt und der Cornell Tech zur Zusammenarbeit in den Themen KI-Sicherheit und Technologie-Governance. Die neue ATHENE Distinguished Lecture Series startete erfolgreich mit Hessens Innenminister Prof. Dr. Roman Poseck – weitere hochrangige Vortragende wie der CISO der hessischen Landesregierung Ralf Stettner, DFKI-CEO Prof. Dr. Antonio Krüger und BSI-Präsidentin Claudia Plattner folgen. Gemeinsam mit führenden KI-Expertinnen und Experten entwickelten Prof. Dr. Michael Waidner und Prof. Dr. Haya Schulmann außerdem eine umfassende Strategie für eine sichere nationale KI-Infrastruktur, und das ATHENE Usable Security and Privacy Lab öffnet seine Türen.

Darüber hinaus erhalten Sie einen Überblick über die ATHENE-Medien-Highlights und einen Ausblick auf kommende Veranstaltungen, darunter die ATHENE-Konferenz "Cybernation Deutschland: Roadmap to Internet Security" am 9. Dezember 2025.

Wir wünschen Ihnen eine informative Lektüre!

Ihr ATHENE-Redaktionsteam

© Catharina Frank

Start der ATHENE Distinguished Lecture Series mit Hessens Innenminister Prof. Dr. Roman Poseck

ATHENE startete eine neue Reihe der ATHENE Distinguished Lecture Series zur Cybersicherheit. Hochrangige Persönlichkeiten aus Wissenschaft, Wirtschaft und Behörden geben Einblicke in aktuelle Cybersecurity-Themen und diskutieren öffentlich über Herausforderungen und Lösungsansätze. Den Auftakt machte am 3. November 2025 der hessische Innenminister Prof. Dr. Roman Poseck mit einem Vortrag zur inneren Sicherheit im digitalen Raum.

Die ATHENE DLS findet monatlich statt. Gemeinsam mit hochrangigen Expertinnen und Experten aus Politik, Behörden und Sicherheitsorganisationen diskutiert Prof. Dr. Haya Schulmann über technologische Entwicklungen, die daraus entstehenden Cybersicherheitsherausforderungen sowie deren Bedeutung für Deutschland und Europa.
Weitere Vortragende sind Hessens CISO Ralf Stettner, die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik (BSI) Claudia Plattner und Prof. Dr. Antonio Krüger, CEO des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI).

Mehr Informationen

Welche Länder (mit mehr als 5 Unis) haben die sichersten UNI-Landschaften?

Cybersicherheit deutscher Universitäten verschlechtert

Der ATHENE-Forschungsbereich Science Shield erhebt und analysiert fortlaufend Daten zur Cybersicherheit im Forschungssektor. Vor wenigen Tagen präsentierte die Leiterin der Studie, Prof. Dr. Haya Schulmann, die erste systematische Langzeitanalyse zur Cybersicherheit von 92 deutschen Universitäten. Die Studie dokumentiert eine dramatische Verschlechterung: Während die Anzahl der Internet-Domänen um 27 Prozent zunahm, verdreifachte sich die Anzahl verwertbarer Schwachstellen von etwa 8.400 im Jahr 2023 auf über 25.200 im Jahr 2025.
Die Analyse zeigt deutliche Unterschiede zwischen Universitäten – große Volluniversitäten mit zentralen IT-Abteilungen weisen signifikant geringere Schwachstellendichten auf als kleinere Spezial- und Privatuniversitäten.
Die Studie identifiziert zentrale Handlungsfelder mit hoher Hebelwirkung: konsequente Inventarisierung, verbindliche Sicherheitsstandards für Dienstleister sowie landesweite IT-Dienste und bundesweit einheitliche Standards.

Mehr Informationen

Strategie für eine nationale KI-Infrastruktur

Gemeinsam mit führenden KI-Expertinnen und Experten von DFKI, hessian.AI, Jülich Supercompting Centre (JSC) sowie den Universitäten TU Darmstadt, Goethe-Universität Frankfurt und Universität des Saarlandes haben Prof. Dr. Michael Waidner und Prof. Dr. Haya Schulmann eine umfassende Strategie für eine nationale KI-Infrastruktur entwickelt. Beim ATHENE Zukunftsforum "Cybernation Deutschland – KI und Cybersicherheit" Ende September wurde sie erstmals der Öffentlichkeit vorgestellt.
Kernpunkte der Strategie sind:

- Aufbau einer nationalen KI-Infrastruktur mit eigenen, wettbewerbsfähigen Basismodellen
- Standardisierung statt föderaler Zersplitterung
- Wissenschaftsbegleitete Entscheiduneng statt Gießkannenprinzip
- Cybersicherheit von an Anfang als integraler Bestandteil
- Gründung einer leistungsfähigen deutschen KI-Agentur mit klarem Mandat zur Umsetzungen

Zur Roadmap

Zur Konferenz

Transatlantische Partnerschaft für digitale Sicherheit

Ein Memorandum of Understanding zwischen der Goethe-Universität Frankfurt und der Initiative for CryptoCurrencies and Contracts (IC3) am Cornell Tech Institut begründet eine verstärkte Zusammenarbeit in der transatlantischen Cybersicherheitsforschung. Die Absichtserklärung verfolgt das Ziel, innovative Forschungsvorhaben voranzutreiben, Lösungsansätze für aufkommende digitale Bedrohungsszenarien zu erarbeiten und dadurch die Sicherheit auf beiden Seiten des Atlantiks zu erhöhen. Die Partnerschaft umfasst schwerpunktmäßig kollaborative Forschung in den Bereichen KI-Sicherheit, Technologien zur Wahrung der Privatsphäre sowie die Erarbeitung von Governance-Rahmenwerken für verantwortungsbewusste Technologieentwicklung. ATHENE-CEO Prof. Michael Waidner betont: „Diese Partnerschaft vereint komplementäre Stärken in Forschung, Anwendung und Richtlinienkompetenz mit dem Ziel, praktische Lösungen für heutige und künftige Cyberbedrohungen zu liefern."

Zur Pressemeldung

Fortschritt bei kryptografischen Schlüsselableitungsfunktionen

Schlüsselableitungsfunktionen (Key Derivation Function, KDF) sind zentrale Komponenten praktischer Verschlüsselungssysteme – sind sie unsicher, ist die gesamte Verschlüsselung unsicher. ATHENE-Forschende der TU Darmstadt haben gemeinsam mit Forschenden der ETH Zürich und IBM das klassische KDF-Sicherheitsmodell aus dem Jahr 2010 grundlegend überarbeitet und zu einem Multi-Input-KDF erweitert. Das neue Modell ermöglicht die Analyse moderner Verschlüsselungsprotokolle und quantensicherer Kryptografie, bei denen verschiedene Geheimnisse aus unterschiedlichen Quellen verarbeitet werden müssen. Die auf der Eurocrypt 2025 veröffentlichte Arbeit führte bereits zu einer Anpassung im KDF-Standard von ETSI.

Mehr Informationen

ATHENE auf Top-Konferenzen erfolgreich

ATHENE-Forschende erzielten bedeutende Erfolge auf zwei internationalen Spitzenkonferenzen für Cybersicherheit und Künstliche Intelligenz. Auf der EMNLP 2025 wurden sechs Paper akzeptiert, darunter CodeSSM – das weltweit erste umfassend getestete State Space Model für Code-Analyse – sowie Arbeiten zur Erkennung von KI-generiertem Code und zur Absicherung von KI-Agenten gegen Manipulationen. Auf der ACM CCS 2025 präsentierten ATHENE-Forschende zwei Paper: eines zu nachverfolgbarer Schwellenwert-Verschlüsselung für Blockchain-Anwendungen und eines zur Sicherheit probabilistischer Datenstrukturen gegen adaptive Angriffe. Die Präsentationen erfolgten im Oktober in Taipei (ACM CCS) und im November in Suzhou (EMNLP).

Paper auf der ACM CCS

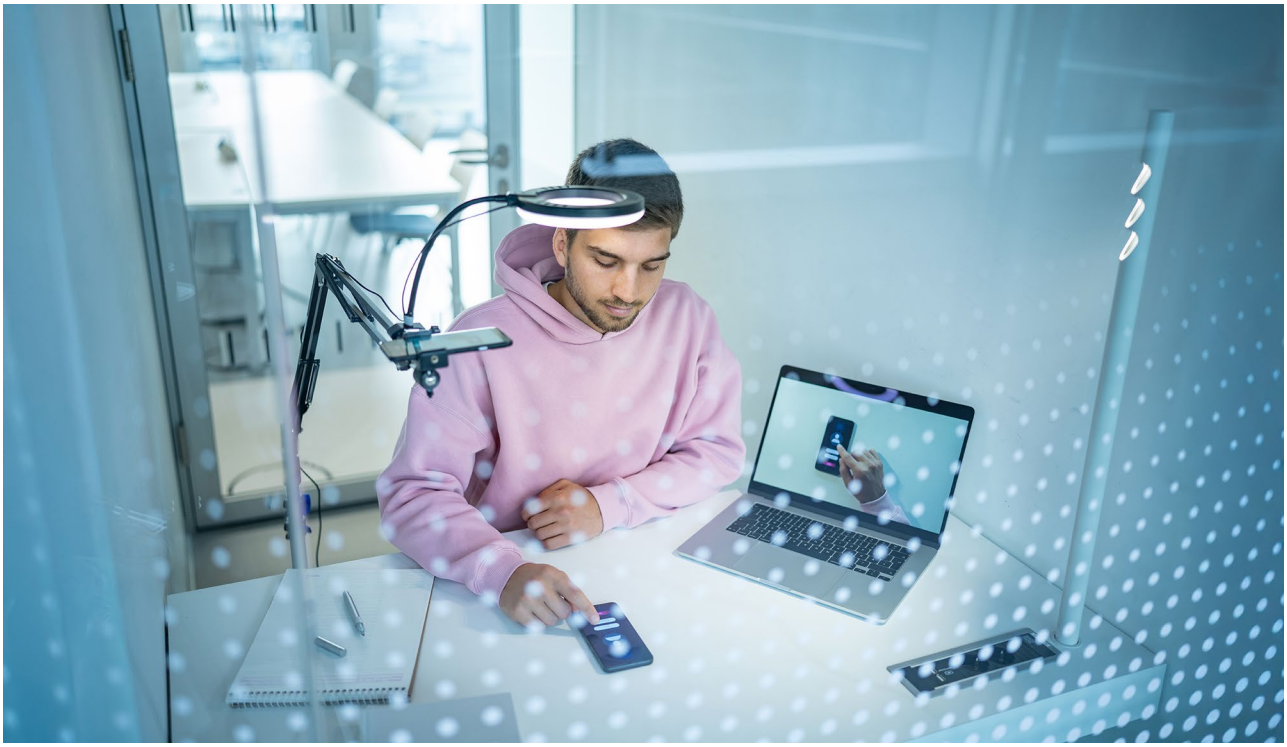
Paper auf der EMNLP

© TU Darmstadt | Paul Glogowski

Aus unserer Forschung: Faire Gesichtserkennung durch kontinuierliche Labels

Prof. Dr.-Ing. Naser Damer entwickelt mit seinem Team in ATHENE neuartige Methoden für faire biometrische Systeme. Anstelle diskreter ethnischer Kategorien verwendet sein Ansatz multi-dimensionale Ethnizitätsscores, die fließende Übergänge und Mischformen abbilden. Die Evaluation von über 65 Gesichtserkennungsmodellen zeigt, dass sich Fairness und Präzision gegenseitig verstärken können. Im Interview erklärt der Leiter des Biometrics Application Lab und der Next Generation Biometric Systems Research Area die Details der Methode und ihre Bedeutung für vertrauenswürdige KI-Anwendungen.

Zum Interview



© Gregor Schuster

Eröffnung des ATHENE Usable Security and Privacy Labs

Das neue ATHENE Usable Security and Privacy Lab (USP-Lab) ist auf die Durchführung von Nutzerstudien zur Gebrauchstauglichkeit und Benutzbarkeit von sicherheits- und datenschutzrelevanten Technologien spezialisiert. Im Fokus stehen Fragestellungen aus dem Bereich User-centered Security and Privacy, insbesondere zu Privatsphäre, menschzentrierten und transparenzerhöhenden Ansätzen. Das USP-Lab steht allen ATHENE-Forschenden zur Verfügung. Auch eine Einbindung im Rahmen von Lehre und Transfer durch ATHENE-Mitwirkende ist möglich. Forschende außerhalb von ATHENE können eine Nutzung des USP-Labs anfragen.
Das USP-Lab verfügt über alle nötigen technischen und methodischen Voraussetzungen, um Usability-Methoden wie Fokusgruppen, User-Interviews, Prototyping, Usability-Tests (am PC und Handy), Surveys, Card-Sorting, Eye-Tracking und andere durchzuführen.

Webseite zum USP-Lab

Über die ATHENE Labs

In ihrem neusten Gastbeitrag in der F.A.Z. analysieren unser CEO Prof. Dr. Michael Waidner und ATHENE-Board-Mitglied Prof. Dr. Haya Schulmann systematisch die Kritik am Einsatz von Palantir Gotham durch deutsche Polizeibehörden. Sie widerlegen technische Sicherheitsbedenken und bestätigen, dass bei sachgemäßem Betrieb kein Datenabfluss erfolgt. Die emotionale Ablehnung aufgrund der Person Peter Thiel basiert nicht auf empirischen Belegen, sondern auf Bauchgefühl. Deutschland zeigt bei kritischeren Abhängigkeiten wie Microsoft Windows oder F-35A deutlich weniger Bedenken.
Zum Gastbeitrag (hinter Paywall): https://www.faz.net/aktuell/wirtschaft/kuenstliche-intelligenz/digitale-souveraenitaet-was-wir-aus-der-debatte-ueber-palantir-lernen-koennen-accg-110772211.html.

Table Media hat ATHENE Board-Mitglied Prof. Dr.-Ing. Mira Mezini als eine von vier Expertinnen und Experten zu ihrer Einschätzung zur digitalen europäischen Souveränität gefragt. In ihrem Statement warnt Mira Mezini vor einem systematischen „Sovereignity Washing" im europäischen Cloud-Bereich: US-Anbieter bewerben ihre Dienste als europakompatibel, obwohl der US CLOUD Act Behörden weiterhin Datenzugriff erlaubt – selbst bei Speicherung in Europa.
Zum Beitrag: https://table.media/ceo/tablestandpunkt/schlagwort-2025-digitale-souveraenitaet

Im November 2024 wurden zwei Datenkabel in der Ostsee durchtrennt, darunter eine Verbindung zwischen Deutschland und Finnland. Die Ermittlungen richten sich gegen ein chinesisches Schiff aus Russland. ATHENE-Wissenschaftler Jonas Franken ordnet diesen Vorfall in der Videoreihe „Was kostet die Welt" produziert von der F.A.Z. für funk – einem Content-Netzwerk von ARD und ZDF – in einen größeren sicherheitspolitischen Kontext ein. In seiner Analyse beschreibt er den Wandel globaler Netzinfrastrukturen durch eigenfinanzierte Kabelprojekte von Technologiekonzernen wie Google, Meta,

Microsoft und Amazon, die Routenwahl und machtpolitische Abhängigkeiten neugestalten. Weiterhin erörtert er, welche Rolle Sabotage-, Spionage- und Kill-Switch-Szenarien in aktuellen sicherheitspolitischen Planungen spielen und wie verwundbar kritische digitale Infrastrukturen gegenüber gezielten Angriffen sind.
Zum Beitrag auf YouTube: https://www.youtube.com/watch?v=fU4b7P1TGBE&list=PPSV

Seit der Veröffentlichung von ChatGPT im November 2022 hat sich die Entwicklung großer Sprachmodelle rasant beschleunigt, ein neues Sprachmodell nach dem anderen wird veröffentlicht. In ihrem Gastbeitrag in der F.A.Z. geben Prof Dr. Iryna Gurevych und ihre PhD-Studentin Irina Bigoulavea einen Überblick über den Stand der derzeit verfügbaren Sprachmodelle und zeigen auf, wie weit die Künstliche Intelligenz heute wirklich ist.
Zum Beitrag (hinter Paywall):
https://www.faz.net/aktuell/wirtschaft/kuenstliche-intelligenz/sprachmodelle-wie-weit-die-kuenstliche-intelligenz-wirklich-ist-accg-110739336.html

---

ATHENE Distinguished Lecture

03.12.2025: ATHENE DLS mit Ralf Stettner, CISO der hessischen Landesregierung, unser Gast. In seiner Keynote spricht er über das "Cybersicherheitsland Hessen".
16.01.2026: ATHENE DLS mit einer Keynote von Prof. Dr. Antonio Krüger, CEO des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) | Professor an der Universität des Saarlandes, zu "KI und Europa und KI Transfer im Allgemeinen".
Mehr Informationen: https://www.athene-center.de/dls

06.12.2025: ATHENE bei der KI-Tour in Darmstadt
Die hessische Digitalministerin Prof. Dr. Kristina Sinemus und der aus Funk und Fernsehen bekannte Moderator Willi Weitzel machen mit der KI-Tour Halt in Darmstadt. Am Samstag, 6.12., haben Bürgerinnen und Bürger im Residenzschloss in Darmstadt Gelegenheit, interaktive Exponate hautnah zu erleben und mit Expertinnen und Experten ins Gespräch zu kommen. ATHENE präsentiert einen interaktiven Fotostand und demonstriert, wie KI-gestützte Bildorganisation durch einfache Eingaben in Alltagssprache funktioniert. Die Live-Demonstration verdeutlicht die Möglichkeiten moderner KI-Programmierung und thematisiert zugleich wichtige Aspekte zu Datenschutz und digitaler Sicherheit.
Mehr Informationen: https://www.athene-center.de/aktuelles/veranstaltungen/athen-bei-der-ki-buergertour-in-darmstadt-1906

9.12.2025: ATHENE Konferenz Cybernation Deutschland: Roadmap to Internet Security
Das Internet ist das Rückgrat unserer modernen Gesellschaft. Unsere kritischen Infrastrukturen, unsere Gesellschaften, Regierungen, die Industrie und die Forschung sind alle auf ein stabiles und sicheres globales Netzwerk angewiesen. Angriffe auf zentrale Komponenten des Internets können landesweite und globale Folgen haben. Die Sicherheit des Internets ist daher ein zentraler Pfeiler der nationalen und internationalen Sicherheit. Vor diesem Hintergrund lädt ATHENE Sie am 9. Dezember in Frankfurt zur Konferenz "Cybernation Deutschland: Roadmap to Internet Security" ein. Diskutieren Sie mit internationalen Expertinnen und Experten über Herausforderungen und Lösungsmöglichkeiten. Die Teilnahme ist kostenfrei, eine Anmeldung erforderlich.
Mehr Informationen: https://www.athene-center.de/roadmap-to-internet-security

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

Impressum

Fraunhofer-Institut für Sichere Informationstechnologie
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
Rheinstraße 75
64295 Darmstadt
Telefon +49 6151 869-368
Fax +49 6151 869-224
E-Mail: pr@athene-center.de

ist eine rechtlich nicht selbstständige Einrichtung der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
Hansastraße 27 c
80686 München
Telefon +49 89 1205- 0
Verantwortliche Redakteurin:
Cornelia Reitz
Telefon +49 6151 869 368