VERANTWORTUNGSVOLLE DIGITALISIERUNG ALS GRUNDLAGE DIGITALER SOUVERÄNITÄT

Vertrauenswürdige Technologien „Made in Austria“ als Basis für eine resiliente Gesellschaft und globale Wettbewerbsfähigkeit

Center for Digital Safety & Security
AIT Austrian Institute of Technology
Deutsche Version

AUSTRIAN INSTITUTE OF TECHNOLOGY

WE MAKE INNOVATION
A DRIVING FORCE
IN EUROPE.

www.ait.ac.at

Vorwort

Digitale Souveränität als neue Notwendigkeit für globale Wettbewerbsfähigkeit und eine demokratische Gesellschaft.

Europäische Systemhersteller:innen, Netzbetreiber:innen und Serviceanbieter:innen stellten bei ihren Digitalisierungsstrategien bisher vor allem Kostensenkungen und Effizienzsteigerungen in den Mittelpunkt. Outsourcing und die Kompetenzverlagerung waren die wichtigsten Mechanismen zur Weiterentwicklung von Unternehmen und öffentlichen Institutionen. Diese Entwicklung führte aber zu grundlegenden Abhängigkeiten von kontinuierlich und günstig verfügbaren digitalen Zulieferprodukten und Anbietern.

Die Wirtschaft steht daher vor der neuen Herausforderung, komplexere und fragile Zulieferökosysteme zu beherrschen, um international wettbewerbsfähig zu bleiben. Digitale Souveränität, also die Fähigkeit zu selbstbestimmtem Handeln, ist zur neuen Voraussetzung für eine funktionierende globale Wirtschaft geworden, bestimmt aber zugleich auch die souveräne Handlungsfreiheit von Staaten. Diese bildet die Grundlage für demokratische, friedfertige Gesellschaftsstrukturen. Darüber hinaus brauchen wir eine klare und stabile Datensouveränität, um der wachsenden Bedeutung und Dominanz von Datensammlungen Rechnung zu tragen. Fehlende Datensouveränität (digitale Autonomie) gefährdet die persönliche Integrität, untergräbt demokratische Strukturen und verhindert die Entstehung neuer datenbasierter Geschäftsmodelle.

Heute speichern und verarbeiten nur wenige Unternehmen den Großteil der globalen Informationssammlungen auf digitaler Ebene – Daten, die den Rohstoff bilden für digitale Geschäftsmodelle und das Training von KI. Diese globalen Infrastrukturen mit Monopolcharakter schränken die Teilhabe vieler Akteur:innen in einem offenen globalen Ökosystem ein und behindern den Wettbewerb. Noch gravierender ist, dass durch diesen Prozess unsere Fähigkeit zur selbstbestimmten Nutzung und Verarbeitung eigener Daten zunehmend eingeschränkt wird.

Gerade im öffentlichen Bereich erfordert digitale Souveränität eine verantwortungsvolle Entwicklung digitaler Lösungen, bei der technologische Leistungsfähigkeit mit rechtlichen, ethischen und gesellschaftlichen Anforderungen in Einklang gebracht wird. Digitale Systeme müssen nicht nur effizient, sondern auch vertrauenswürdig, nachvollziehbar und sicher gestaltet sein.

Nur wenn Datenschutz, Transparenz, Resilienz und demokratische Grundwerte von Beginn an integriert werden, kann die Digitalisierung ihre volle Wirkung entfalten und das Vertrauen sowohl der Bürger:innen als auch der Wirtschaft und Institutionen stärken.

Daraus folgt insbesondere für staatliche und hoheitliche Anwendungen eine besondere Verantwortung: Digitale Systeme dürfen nicht allein nach den Gesichtspunkten der Effizienz gestaltet werden, sondern müssen auch strategische Resilienz, Rechtskonformität sowie ethische Maßstäbe und gesellschaftliche Auswirkungen systematisch berücksichtigen. Nur so entstehen tragfähige Infrastrukturen, die Sicherheit gewährleisten, demokratische Prinzipien schützen und die langfristige Handlungsfähigkeit des Staates sichern.

Innovation entsteht dabei aus dem notwendigen Zusammenspiel von Technologieherstellern, Anbietern, der Industrie, der Forschung und den Behörden. Erst durch diese enge Kooperation werden tragfähige und skalierbare Lösungen möglich, die nicht nur national wirksam sind, sondern sich auch auf dem globalen Parkett durchsetzen können. Digitale Souveränität erfordert daher ein starkes Innovationsökosystem, das die höchstmögliche Qualität im technologischen Sinn mit strategischer Zusammenarbeit verbindet.

Als Konsequenz daraus benötigen wir unbedingt Kompetenzen, um die Vertrauenswürdigkeit und Integrität technischer Systeme beurteilen und nachhaltig sichern zu können. Dabei geht es nicht um Protektionismus oder vollständige Eigenentwicklungen, sondern um die Sicherung einer grundlegenden Handlungsfreiheit, die es im Notfall oder aus strategischen Gründen erlaubt, auf Alternativen zurückgreifen zu können, entsprechend der zentralen Funktion freier Wirtschaftssysteme.

Die EU-Kommission trägt dieser Dynamik mit speziellen EU-Innovations- und Forschungsprogrammen zur Stärkung digitaler Souveränität Rechnung, um strategische Technologien und Kompetenzen wie KI, Cybersicherheit, Quantentechnologien und Mikrochips in der EU global konkurrenzfähig zu etablieren. Weiters setzt die EU auf eine neue Datenstrategie und schafft mit Data Act, Data Governance Act und dem AI Act klare, rechtlich bindende Regeln für Transparenz, souveräne Datenverarbeitung und fairen Datenhandel.

Für eine starke, souveräne Wirtschaft und zur effektiven Umsetzung der Innovationsprogramme der Europäischen Kommission sind starke Forschungs- und Technologieorganisationen erforderlich, die als neutrale Innovationsinfrastruktur für Industrie, öffentliche Hand sowie Wissenschaft wirken und europäische Schlüsseltechnologien wettbewerbsfähig zur Anwendung bringen.

Weiters entsteht zunehmend eine Dynamik, gemeinschaftlich geschaffene, öffentlich finanzierte oder industriell entwickelte Open-Source-Technologien breiter in Unternehmen und der öffentlichen Verwaltung einzusetzen. Vor allem durch die EU-Industrie wird mit der Open-Source- und Standardisierungsinitiative Gaia-X eine Grundlage geschaffen, um neue Datenmärkte (Datenräume) im globalen Kontext zu etablieren, die auf verteilte Datenhaltung aufbauen und einen sicheren und vertrauenswürdigen Datenaustausch ermöglichen.

Wenn wir diese neuen Ansätze selbstbewusst aufgreifen und unsere IT-Systeme durch europäische Innovation resilienter gestalten, sichern wir unsere selbstbestimmte Handlungsfreiheit und stärken nachhaltig Wirtschaft und Gesellschaft. So erreichen wir globale Wirtschaftsbeziehungen auf Augenhöhe.

Helmut Leopold
Head of Center for Digital Safety & Security
AIT Austrian Institute of Technology

Einleitung

Das AIT Austrian Institute of Technology ist mit mehr als 1.600 Beschäftigten Österreichs größte Forschungs- und Technologieorganisation und fokussiert auf die Forschungsschwerpunkte „Nachhaltige und resiliente Infrastrukturen“, insbesondere in den Bereichen Energie, Transport und Gesundheit, sowie die „Digitale Transformation von Industrie und Gesellschaft“. Dabei arbeitet das AIT eng mit Universitäten, der Industrie und öffentlichen Institutionen zusammen. Durch die Forschung und die technologischen Entwicklungen am AIT werden grundlegende Innovationen für die nächste Generation von Infrastrukturtechnologien in den Bereichen Energy, Transport Technologies, Health & Bioresources, Digital Safety & Security, Vision, Automation & Control sowie Technology Experience verwirklicht. Ergänzt werden diese wissenschaftlichen Forschungsgebiete um die Kompetenz im Bereich Innovation Systems & Policy. Gesellschafter des AIT sind die Republik Österreich (Bundesministerium für Innovation, Mobilität und Infrastruktur – BMIMI), die 50,46 % der Anteile hält, und der Verein zur Förderung von Forschung und Innovation (Industriellenvereinigung Österreich) mit 49,54 % der Anteile.

Center for Digital Safety & Security

Im AIT Center for Digital Safety & Security arbeiten über 230 Expert:innen an modernsten Informations- und Kommunikationstechnologien, um diese im Kontext der umfassenden Digitalisierung und globalen Vernetzung hochsicher und zuverlässig entwickeln sowie nutzen zu können.

Das Center leistet heute mit seiner Fokussierung auf zentrale Schlüsseltechnologiefelder wie Cyber Security, Data Science & Künstliche Intelligenz (KI), Quanten- und Photonik-Technologien, Software für sicherheitskritische Systeme, digitale Krisen- und Katastrophenmanagementsysteme, sichere Software und smarte Sensorsysteme sowie höchst zuverlässige Funksysteme der nächsten Generation wesentliche Beiträge zur nationalen und europäischen Digitalisierungsstrategie. Ergänzt wird diese technologische Kompetenz durch eine besondere Industrialisierungskompetenz, die den Transfer innovativer Forschungsergebnisse in marktfähige Lösungen unterstützt. In diesen digitalen Schlüsseltechnologiebereichen konnte das AIT eine erfolgreiche internationale Führungsposition erreichen. Es unterstützt damit maßgeblich die Zielsetzung der EU zur Sicherstellung einer hohen digitalen Souveränität in Europa und agiert heute für Österreich als wichtiger Treiber für eine positive Entwicklung eines nationalen Digitalisierungsökosystems.

Auf dieser Basis adressiert das Center for Digital Safety & Security unterschiedliche Märkte, wie unter anderem die Halbleiterindustrie, den Automotive-Sektor, Betreiber von kritischen Infrastrukturen wie Energienetze und Kraftwerke, Finanzmärkte, oder auch den Sicherheitsbereich im Kontext des Schutzes kritischer Infrastrukturen, sowie Umweltmonitoring und Krisen- und Katastrophenmanagement. In enger Kooperation mit Wirtschaft und Industrie, Wissenschaft und öffentlicher Hand erfolgt eine strategische Technologieforschung mit der Entwicklung von Prototypen bis hin zur Validierung von Anwendungen.

Im Bereich der nationalen Community für Sicherheitsforschung besitzt das Center for Digital Safety & Security eine anerkannte Position als der wichtigste Stakeholder und Gestalter für die Umsetzung der nationalen Forschungsstrategie für digitale Sicherheit in den nationalen Programmen KIRAS, K-PASS und FORTE, um Behörden, Industrie, KMU, Forschung und Sozialwissenschaften zusammenzubringen und die Wettbewerbsfähigkeit österreichischer Organisationen für Aktivitäten im EU-Ökosystem zu stärken. Im internationalen Sicherheitsforschungskontext konnte das Center eine führende Rolle im Vergleich mit den anderen EU-RTOs (Research and Technology Organisations) erreichen und in Rankings bezüglich erfolgreicher EU-Projekte eine Spitzenposition einnehmen und damit wesentlich dazu beitragen, dass der österreichische High-Tech-Industriestandort durch Kooperationen mit nationalen Behörden wie dem Bundesministerium für Landesverteidigung (BMLV) sowie dem Bundesministerium für Inneres (BMI) und dem Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) auch auf internationaler Ebene eine wesentliche Sichtbarkeit erreichen konnte.

Um als integraler Bestandteil eines internationalen Innovationsökosystems im Bereich der digitalen Sicherheitsforschung zu agieren, etablierte das Center mit dem International Digital Security Forum (IDSF) erfolgreich ein globales Dialogforum in Wien. Das IDSF ist ein wichtiges Konferenz-Flaggschiff, das in enger Zusammenarbeit

mit österreichischen Behörden wie dem Bundesministerium für europäische und internationale Angelegenheiten (BMEIA), dem Bundeskanzleramt (BKA), dem Bundesministerium für Inneres (BMI) und dem Bundesministerium für Landesverteidigung (BMLV) sowie der Wirtschaftskammer Österreich (WKO) und dem Kompetenzzentrum Sicheres Österreich (KSÖ) entwickelt wurde. Es gibt österreichischen Anbietern sowie kleinen und mittleren Unternehmen (KMU) im digitalen Sicherheitsbereich die Möglichkeit, sich auf einem internationalen Markt zu präsentieren. Weiters gründete das Center die international ausgerichtete „PeaceTech Alliance", um den globalen multidisziplinären Diskurs und die Entwicklung von Governance-Strukturen für kritische Digitalisierungsentwicklungen zu fördern.

Das AIT gilt mit dem Center for Digital Safety & Security heute als global akzeptierte Brand für digitale Sicherheitskompetenz. Das Center kooperiert beispielsweise eng mit der Internationalen Atomenergiebehörde (IAEA), dem World Institute for Nuclear Security (WINS), dem Vienna Center for Disarmament and Non-Proliferation (VCDNP) sowie dem UN-Office of Counter-Terrorism (UNOCT).

Zur Unterstützung der Datensouveränitätsziele in der EU und zur Förderung der Entwicklung eines neuen datengetriebenen Ökosystems hat das Center zudem im gemeinsamen Auftrag des Bundesministeriums für Innovation, Mobilität und Infrastruktur (BMIMI) und des Staatssekretariats für Digitalisierung im Bundeskanzleramt (BKA) erfolgreich und maßgeblich den Gaia-X Hub Austria zur Beschleunigung europäischer Datenökosysteme für ökonomische, ökologische und gesellschaftliche Wertschöpfung vorangetrieben. Durch die besondere Konzeption des nationalen Hubs rund um eine breite Verankerung bei vielen Stakeholdern in Österreich und die verfolgte Strategie, ist das AIT heute erfolgreich als ein EU-Best-Practice-Beispiel zum Aufbau einer EU-weiten Datentechnologiekompetenz positioniert. Die Schaffung von föderierten Datenräumen ist eine wichtige Grundlage für die Umsetzung von datengetriebenen Geschäftsmodellen in allen relevanten Märkten der Industrie sowie der öffentlichen Hand.

Die folgenden Seiten geben einen kompakten Einblick in die thematischen Schwerpunkte aus Forschung und Entwicklung und präsentieren ausgewählte technologische Kompetenzen sowie ausgewählte Lösungen ebenso wie Initiativen des Centers. Sie zeigen auf, wie angewandte Forschung am AIT gemeinsam mit Partnern aus Wirtschaft, Verwaltung und Gesellschaft konkrete Mehrwerte schafft, die von der strategischen Technologieentwicklung über die prototypische Umsetzung bis hin zur praxisnahen Validierung reichen. Das Ziel ist, Kund:innen und Stakeholder:innen ein klares Bild davon zu vermitteln, wie das Center for Digital Safety & Security des AIT Austrian Institute of Technology sie bei aktuellen und zukünftigen Herausforderungen in den Bereichen digitale Sicherheit, Resilienz sowie technologische, datengetriebene und digitale Souveränität unterstützen kann.

Digital Safety & Security

Inhalt

4 **Vorwort**
6 **Einleitung**

10 1. Cyber Security

11 **Cyber Threat Intelligence & Schutz durch KI**
12 Open Source Intelligence (OSINT) Tool „Taranis AI“
12 Machine-Learning-based Intrusion Detection mit „AECID“
12 Systematische Wirksamkeitsprüfung von Erkennungssystemen mittels „Stealth-Cup“

13 **Safety & Security by Design**
14 Cyber Security by Design Tool „ThreatGet“

15 **Post-Quanten Kryptographie**

16 **Services und Dienstleistungen**
16 AIT Cyber Range – Training Center
17 Penetration Testing & Red Teaming
17 Security Consulting

18 2. Data Science & Artificial Intelligence

19 **Kampf gegen Desinformation und Betrug**
20 AIT Media Intelligence Plattform
20 DisDETECT – Plattform zur Erkennung und Analyse von Desinformation
20 Fake-Shop Detector

21 **Knowledge Management**

22 3. Digitales Identitätsmanagement

23 **Biometrische Sensorlösungen**
23 Face-Snap – mobile Erfassung biometrischer Gesichtsprofile
23 Touchless Four Fingerprint (T4F) Scanner

24 4. Schutz kritischer Infrastrukturen

25 fiberRAIL® – Distributed Acoustic Sensing (DAS)
26 Optische Sensorik – FrontierSense

27 5. Krisen- und Katastrophenmanagement

28 **Lagebild & CBRNe**
29 Softwareplattform Horus3D
29 Software-Modul RaptoR
29 Software-Framework MuFASA

30 6. Sustainable & Resilient Society

31 **Digitale Lösungen zum Schutz der Umwelt**
32 AIRDB – Intelligente Lösung zur Luftqualitätsmessung
32 EMIKAT – Komplettlösung zur Verwaltung und Analyse von Emissionsdaten

33 **Smarte Städte & Kommunen**
33 Datenaustausch
33 Wissensmanagement
34 Marktplatz
34 Reporting & Digital Twin

35 7. Enabling Digital Technologies

36 Chip-Technologien der nächsten Generation
37 Quantenverschlüsselung
38 Funktechnologien der nächsten Generation

39 8. Initiativen und Plattformen

40 Gaia-X Hub Austria
41 International Digital Security Forum (IDSF)
42 PeaceTech Alliance

43 9. Internationales Netzwerk

45 10. Ausgewählte Forschungsinfrastrukturen

46 Photonics & Quantum Communication Laboratory
46 Radio Frequency Laboratory
47 AIT Cyber Range – Test & Training Center

48 11. Zertifizierungen

49 **Impressum**

1 CYBER SECURITY

Als nationales Kompetenzzentrum für Cybersicherheit und internationale Anlaufstelle rund um Training und Ausbildung sowie für modernste digitale Werkzeuge für die Cybersicherheit, verfügt das Center for Digital Safety & Security des AIT über jahrzehntelange Erfahrung im Bereich des Schutzes von Steuerungssystemen in kritischen Infrastrukturen und betreibt heute die hybride und flexibel anpassbare IT-Simulationsumgebung „AIT Cyber Range“, auf der internationale Cybersicherheitstrainings durchgeführt werden. In Kombination mit der Entwicklung modernster Tools und Methoden, die dem „Security & Privacy by Design-Ansatz“ folgen, setzen sich die Expert:innen für höchste Computersicherheit ein und heben den verantwortungsvollen Einsatz von Technologie über rein technische oder wirtschaftliche Ziele. Zudem unterstützt das Center die Ziele der nationalen Cyber-Sicherheitsstrategie ganz wesentlich durch neue Lösungen sowie durch die Entwicklung von Fähigkeiten.

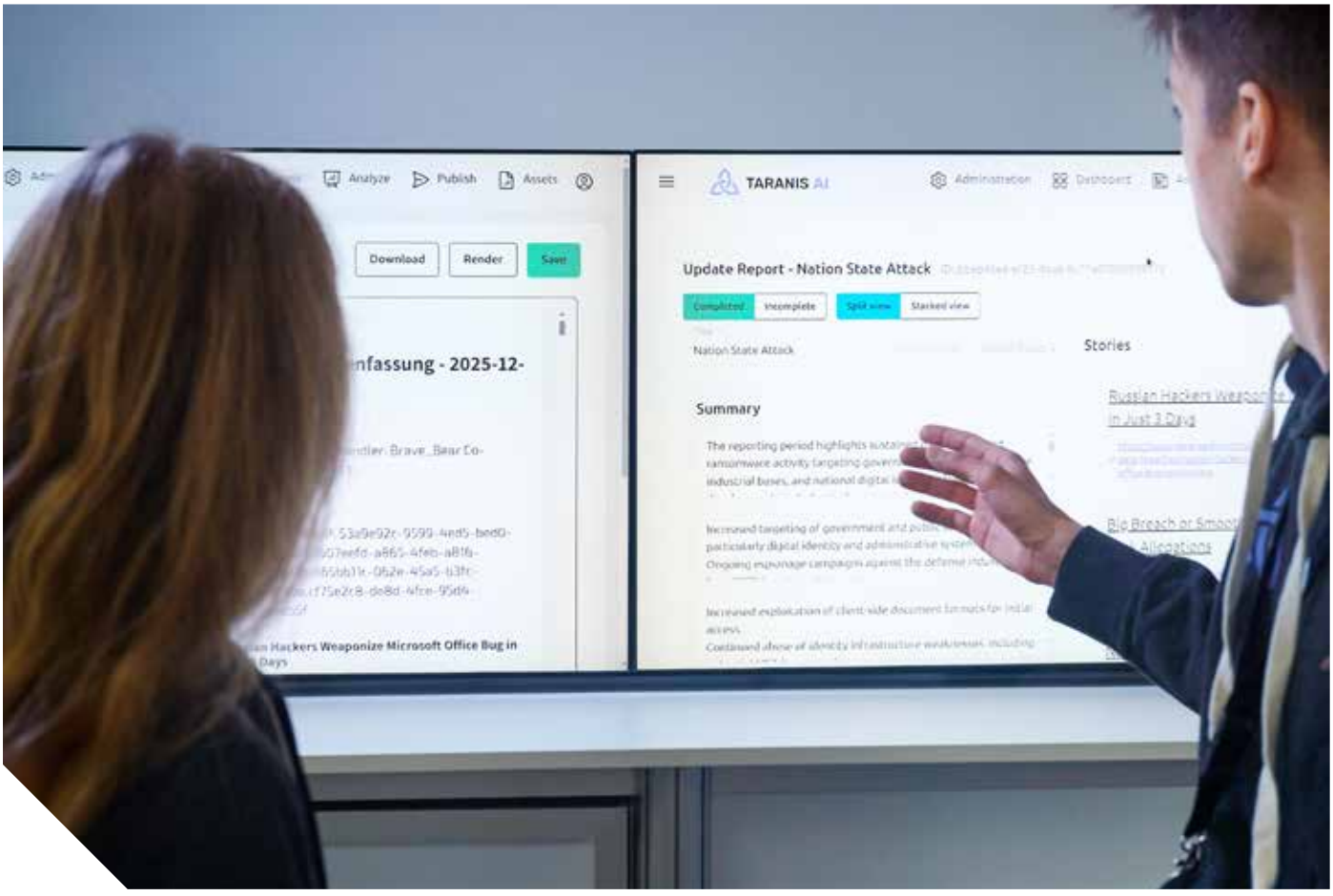
Cyber Security

Cyber Threat Intelligence & Schutz durch KI

Jeden Tag sind Unternehmen und Organisationen gefährlichen Cyberattacken ausgesetzt. Im Kampf gegen diese Bedrohungen müssen Datensicherheitsexpert:innen die jeweilige Situation laufend überwachen, Schlüsselindikatoren festlegen, rasch auf Probleme reagieren und stets über die neuesten Angriffsvektoren, Methoden und Bedrohungen informiert sein. All das gleichzeitig zu bewerkstelligen, ist jedoch oft ein aussichtsloses Unterfangen.

Das Center arbeitet an neuartigen Intrusion Detection Systemen (IDS), die unter Einsatz von Machine Learning das Systemverhalten charakterisieren und Abweichungen von einem festgelegten Ausgangszustand entdecken können. Mit Hilfe dieser Lösungen zur adaptiven Verarbeitung von Netzwerk-Log-Streams können häufig auftretende Muster in Logfiles erkannt, klassifiziert und geclustert werden, um schließlich bekannte normale Aktivitäten von unbekannten schädlichen Aktivitäten in betrieblichen IT-Infrastrukturen zu unterscheiden – ein selbstlernender Ansatz mit minimalem manuellem Konfigurationsaufwand.

Durch die effektive Verknüpfung mit Lösungen zur Gefahrenerkennung kann das System zur Anomalieerkennung individuell konfiguriert und auf die jeweiligen Bedrohungsbereiche ausgerichtet werden. Umgekehrt lassen sich durch die Extraktion von Indikatoren aus rohen Logdaten Informationen über potenzielle Bedrohungen mit einem Minimum an eingesetztem Personal gewinnen.



Taranis AI

Open Source Intelligence (OSINT) Tool „Taranis AI“

Taranis AI ist ein fortschrittliches Open Source Intelligence Tool (OSINT), das künstliche Intelligenz nutzt, um die Informationsbeschaffung und Situationsanalyse zu revolutionieren. Es bietet leistungsfähige OSINT-Funktionen zur automatisierten Analyse großer Mengen unstrukturierter Nachrichtenquellen.

Mithilfe von Künstlicher Intelligenz sowie Natural Language Processing werden relevante Inhalte aus unterschiedlichen Datenquellen gesammelt, angereichert und qualitativ aufbereitet. Eine analyst:innenfreundliche Workflow-Umgebung ermöglicht es, Rohinformationen effizient in strukturierte Berichte zu überführen und bedarfsgerechte Endprodukte, etwa strukturierte Reports oder PDF-Dossiers zu erstellen.

Ergänzt wird dies durch nahtlose Publikationsfunktionen sowie experimentelle Möglichkeiten zur kollaborativen Threat-Intelligence-Zusammenarbeit, etwa über den Austausch auf Story-Ebene via MISP (Malware Information Sharing Platform), einer Open-Source-Softwarelösung zum Sammeln, Speichern, Verbreiten und Teilen von Indikatoren und Bedrohungen im Bereich der Cybersicherheit.

AECID

Machine-Learning-based Intrusion Detection mit „AECID“

Die Abkürzung AECID steht für „Automatic Event Correlation for Incident Detection“ und bezeichnet eine Machine-Learning-basierte Methode zur automatischen Erkennung von Sicherheitsvorfällen. Durch die kontinuierliche Analyse von Systemereignissen in Logdaten sowie die Anwendung spezieller mathematischer Verfahren kann AECID normales von anomalem Verhalten in komplexen Rechnernetzen unterscheiden.

Im Gegensatz zu herkömmlichen Ansätzen benötigt der Algorithmus keine detaillierten Vorkenntnisse über die zu überwachenden IT-Systeme. Stattdessen erkennt AECID nach einer Lern- und Beobachtungsphase eigenständig Muster im Systemverhalten. Grundlage dafür ist ein selbstlernender Algorithmus, der typische Abläufe identifiziert und Abweichungen davon automatisch erkennt.

Die am AIT entwickelte AECID-Technologie passt sich kontinuierlich an neue Situationen an und kommt ohne aufwändige Systemmodellierung oder komplexes Konfigurationsmanagement durch den Betreiber aus. Durch die fortlaufende Aufnahme und Analyse neuer Informationen erweitert und verfeinert AECID seine Wissensbasis kontinuierlich und gewinnt immer präzisere Erkenntnisse über das jeweilige Einsatzsystem.

Stealth-Cup

Systematische Wirksamkeitsprüfung von Erkennungssystemen mittels „Stealth-Cup“

Intrusion-Detection-Systeme (IDS) sind zentrale Bausteine für einen modernen Cyber-Security-Schutz durch die Erkennung von Angriffen in modernen Computernetzwerken. Dennoch bleibt ihre tatsächliche Wirksamkeit, insbesondere unter realen Betriebsbedingungen, schwer messbar. Die Stealth-Cup-Methodik ist ein am AIT entwickeltes, international einzigartiges Forschungs- und Evaluierungskonzept, das realistische, mehrstufige Cyberangriffe in einer vollständig automatisierten IT/OT Cyber Range ermöglicht. Der Ansatz schafft die Grundlage für realitätsnahe und reproduzierbare Bewertungen von Intrusion-Detection-Systemen (IDS) in großen IT/OT Systemen.

Die Führungsrolle des AIT im Bereich realitätsnaher IDS-Evaluierung zeigt sich in mehreren klaren Indikatoren. Die Infrastruktur wurde mit Infrastrukturunternehmen entwickelt und validiert, was ihre Relevanz und Praxistauglichkeit belegt. Der Stealth-Cup bietet eine europaweit einmalige Kombination aus vollständig reproduzierbarer „Infrastructure as Code (IaC)“-basierter Testumgebung und realitätsnahen, durch menschliche Angreifer erzeugten Angriffsmustern. Durch die Bereitstellung unabhängiger, wissenschaftlich belastbarer Evaluierungs- und Testmöglichkeiten unterstützt das AIT die europäische Kompetenz, sicherheitskritische Technologien transparent und evidenzbasiert zu bewerten und trägt so dazu bei, Europas Fähigkeit zu stärken, moderne Erkennungssysteme realitätsnah zu evaluieren und robuste Verteidigungsmechanismen aufzubauen. Stealth-Cup adressiert europäische Behörden, Organisationen und Hersteller insbesondere im Bereich Detection Engineering und Ausbildung von Personal.

Safety & Security by Design

Mit der zunehmenden Digitalisierung von Industrieprozessen wächst der Bedarf an sicheren Entwicklungsansätzen, um Schwachstellen bereits in der Entstehung von IT/OT Systemen zu minimieren und die Wettbewerbsfähigkeit von Unternehmen zu stärken. Denn traditionelle Sicherheitsmaßnahmen greifen üblicherweise erst nach der Entwicklung von IT/OT Systemen, was potenzielle Schwachstellen unentdeckt lässt und die Gefahr von Cyberangriffen erhöht. Insbesondere Industrieunternehmen benötigen daher effektive Methoden, um Sicherheitslücken frühzeitig zu identifizieren und zu schließen. Gleichzeitig müssen internationale Standards eingehalten werden, um die Wettbewerbsfähigkeit auf dem globalen Markt zu sichern.

Diese Anforderungen gewinnen zusätzlich an Bedeutung, da moderne digitale Systeme zunehmend autonom agieren und auf künstlicher Intelligenz basieren – etwa in der industriellen Automatisierung, in vernetzten Produktionsanlagen oder in sicherheitskritischen Anwendungen. KI-gestützte Systeme treffen Entscheidungen immer häufiger selbstständig und in Echtzeit. Damit steigen nicht nur Effizienz und Leistungsfähigkeit, sondern auch die Anforderungen an die Zuverlässigkeit, Nachvollziehbarkeit sowie das kontrollierbare Systemverhalten. Unbeabsichtigte oder unerwünschte Reaktionen solcher Systeme können erhebliche sicherheitstechnische, wirtschaftliche und rechtliche Folgen haben.

Vor diesem Hintergrund hat das Center for Digital Safety & Security am AIT ergänzend zur etablierten Cyber-Security-Expertise gezielt Kompetenzen für „Safety & Security by Design“ aufgebaut. Ziel ist es, Sicherheits- und Zuverlässigkeitsanforderungen systematisch von Beginn an in den Entwicklungsprozess digitaler und KI-basierter Systeme zu integrieren und diese nicht erst im Nachhinein zu prüfen. Ein besonderer Fokus liegt dabei auf Methoden, die auch mit der Komplexität, Unsicherheit und Adaptivität moderner KI-Systeme umgehen können.

Die Expert:innen des Centers entwickeln und erproben hierfür strukturierte Entwicklungs-, Test- und Verifikationsansätze, die eine durchgängige Qualitätssicherung über den gesamten Lebenszyklus digitaler Systeme ermöglichen, beginnend von der Konzeption über den Betrieb bis hin zur Weiterentwicklung. Dabei werden auch die Einsatzgrenzen und Betriebsbedingungen (Operational Design Domains) klar definiert, um sicherzustellen, dass Systeme nur innerhalb jener Rahmenbedingungen agieren, für die sie ausgelegt und überprüft wurden. Auf dieser Basis haben die Expert:innen mit der innovativen Security by Design Entwicklungstechnik ThreatGet eine international anerkannte Methode entwickelt, die Unternehmen dabei unterstützt, Sicherheitsanforderungen frühzeitig, systematisch und standardkonform umzusetzen. Die Spezialist:innen des Centers nehmen zudem eine führende Rolle in der internationalen Standardisierung (IEC, ISO) ein und tragen damit aktiv zur Weiterentwicklung regulatorischer Rahmenbedingungen bei, etwa im Zusammenhang mit dem Cyber Resilience Act. Dadurch leistet das AIT Center einen wesentlichen Beitrag zur sicheren Einführung komplexer digitaler und KI-basierter Systeme und zur nachhaltigen Stärkung der Wettbewerbsfähigkeit österreichischer Industrieunternehmen.

Dependable Systems Engineering

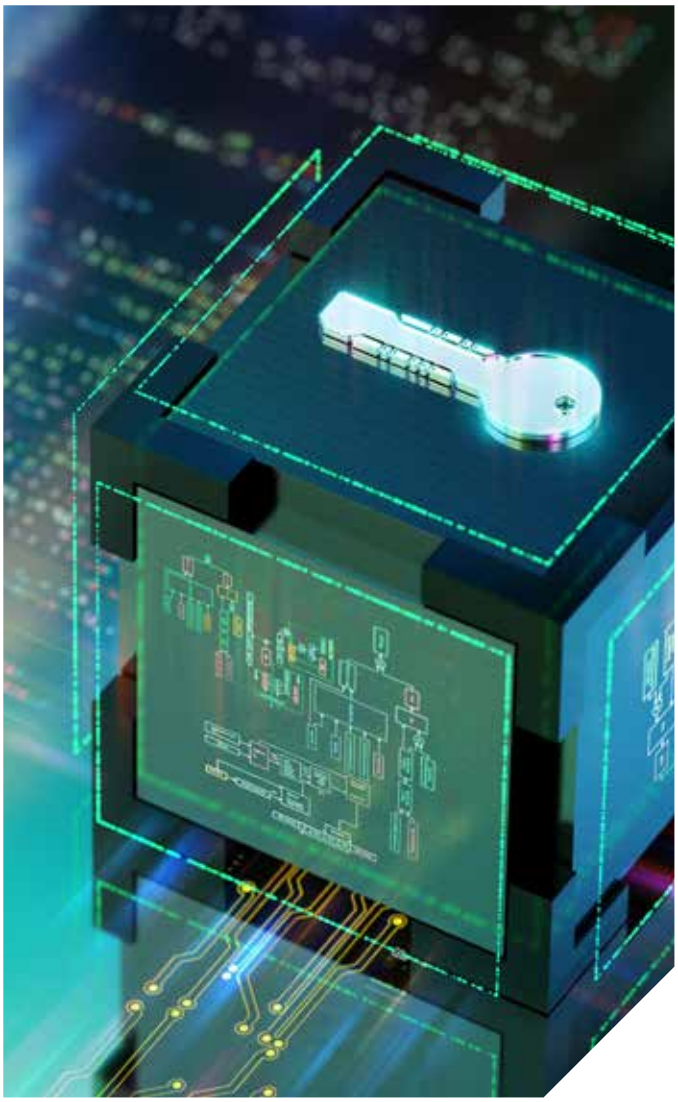
ThreatGet

Cyber Security by Design Tool „ThreatGet“

Mit dem preisgekrönten Sicherheitstool ThreatGet, das auf künstlicher Intelligenz basiert, lässt sich die gesamte Systemarchitektur sicherheitskritischer Anwendungen, wie beispielsweise vernetzter Fahrzeuge, analysieren. Die automatisierte Analyse potenzieller Systemrisiken und Angriffswege kann bereits zu Beginn der Systementwicklung problemlos durchgeführt werden. Dieses Cyber Security by Design Tool ist ein Muss für Branchen mit sicherheitskritischer Infrastruktur, die gemäß den gesetzlichen Vorschriften ein geeignetes Cybersicherheits-Managementsystem einrichten müssen. ThreatGet erhielt 2021 den Constantinus Award in der Kategorie „Digitalisierung/IoT“ und wurde 2022 für den Österreichischen Staatspreis für Beratung in der Kategorie „Managementberatung und IT“ nominiert.

Post-Quanten Kryptographie

Durch die fortschreitende Entwicklung von kryptographisch relevanten Quantencomputern entsteht der Bedarf an Methoden, welche die Integrität, Authentizität, und Vertraulichkeit von Daten auch in einer „Post-Quantum-Welt“ langfristig und beweisbar garantieren. „Quantum-Computer Safe“ Technologien sind Verschlüsselungsverfahren, die auch nach der Verfügbarkeit von Quantencomputern durch diese nicht entschlüsselt werden können.



Die Kryptographie-Gruppe des Center for Digital Safety & Security am AIT setzte in den letzten Jahren einen entsprechenden Forschungsschwerpunkt, um das AIT innerhalb Österreichs, aber auch im europäischen und internationalen Kontext, als Kompetenzzentrum für post-quanten-sichere Kryptographie (PQC) zu etablieren. Dort werden Verfahren entwickelt, die in einer sogenannten „Post-Quantum-Welt“ mit leistungsfähigen Quantencomputern weiterhin beweisbare Sicherheitsgarantien für Daten geben können. In enger Zusammenarbeit mit Expert:innen für Quantenverschlüsselung des Centers arbeitet das Team an einer Hybridisierung von post-quanten-sicheren Verfahren mit Quanten-Schlüsselverteilung (QKD), um die physikalischen Sicherheitsgarantien von QKD mit den Ende-zu-Ende-Sicherheitsgarantien von PQC zu kombinieren. Das gewonnene Know-how aus allen Ebenen wird parallel dazu aktiv im Bereich der europäischen und internationalen Standardisierung eingebracht.

Als Koordinator von Projekten wie PREPARED (KIRAS), AUTKRYPTO (K-PASS), oder QCI-CAT (Digital Europe Programme) sowie als Partner in Projekten wie POSEIDON (Horizon Europe) hat sich das Team als verlässlicher Partner und zentrale Anlaufstelle für Post-Quanten-Forschung für österreichische Bedarfsträger und darüber hinaus etabliert. Die Migration bestehender komplexer Systeme wurde beispielsweise im Zuge des KIRAS-Projekts PREPARED demonstriert, in dem gemeinsam mit dem Bundeskanzleramt sowie weiteren Partnern aus Industrie und Wissenschaft die PDF-Signaturlösung der ID Austria prototypisch in eine post-quanten-sichere Version übergeführt wurde.

KIRAS

PREPARED

QCI-CAT

POSEIDON

Post-Quanten Kryptographie

Services und Dienstleistungen

Praxisnahe Cyber Security Services unterstützen Organisationen dabei, ihre digitale Resilienz entlang des gesamten Security-Lifecycles nachhaltig zu stärken. Das Spektrum reicht von realitätsnahen Trainings- und Simulationsumgebungen mit der AIT Cyber Range über technische Sicherheitsüberprüfungen und Penetrationstests bis hin zu strategischer Security-Beratung zur Absicherung moderner digitaler Systeme, Prozesse und kritischer Infrastrukturen.

AIT Cyber Range – Training Center

Im Kontext des Ausbaus der EU-weiten Cyber-Security-Fähigkeiten und der Entwicklung von speziellen beruflichen Weiterbildungsprogrammen für Behörden, kritische Infrastrukturbetreiber und KMU gilt das AIT mit dem Center for Digital Safety & Security heute international als führender Stakeholder. In enger Kooperation mit internationalen Partnern wie beispielweise der Internationalen Atomenergiebehörde (IAEA), dem World Institute for Nuclear Security (WINS), dem Vienna Center for Disarmament and Non-Proliferation (VCDNP), sowie dem UN Office of Counter-Terrorism (UNOCT) führt das AIT Center weltweit Schulungen durch.

Im Zeitalter zunehmender digitaler Bedrohungen und globaler Vernetzung ist die Sicherung kritischer Infrastrukturen essenziell, um nationale und internationale Stabilität zu gewährleisten. Cyber Security ist deshalb ein international wichtiger Forschungsbereich, sowohl für die Entwicklung effektiver Abwehrtechnologien als auch zum Aufbau von Verteidigungs- und Abwehrfähigkeiten in Organisationen, die auch bei staatlichen Sicherheitsstrukturen im Einsatz sein können. Mit der wachsenden Abhängigkeit von digitalen Systemen steigt das Risiko von Cyberangriffen auf kritische Infrastrukturen wie Energieversorgung, Gesundheitswesen, Transportnetzwerke oder Ministerien enorm. Diese Angriffe können nicht nur wirtschaftliche Schäden verursachen, sondern auch die öffentliche Sicherheit und das Vertrauen in staatliche Institutionen gefährden. Es besteht ein dringender Bedarf an praxisnahen, innovativen Trainingsmethoden, um IT-Sicherheitsexpert:innen, Betreiber kritischer Infrastrukturen und Security Operations Centers (SOC) auf die Erkennung, Analyse und Reaktion auf aktuelle und zukünftige Bedrohungsszenarien vorzubereiten.

Am AIT wurde daher im Center for Digital Safety & Security mit der AIT Cyber Range eine innovative Simulationsumgebung zur realitätsnahen Nachbildung von IT- & OT-Netzwerken in sicherheitskritischen Umgebungen (Digital Twin) aufgebaut. Diese wird für das Abwehrtraining von Cyberattacken auf kritische Infrastrukturen und Unternehmensnetzwerke herangezogen und in Kombination mit maßgeschneiderten Ausbildungsangeboten für Betreiber kritischer Infrastrukturen, Behörden und KMU weltweit angeboten. Ein besonderer Schwerpunkt liegt dabei auf Trainings zum Aufbau und Betrieb von Security Operations Centers (SOC), einschließlich Schwachstellenmanagement, Bedrohungsanalyse sowie der Reaktion auf Cybervorfälle unter realitätsnahen Bedingungen.

Zu den Referenzkunden zählen hier das World Institute for Nuclear Security (WINS), United Nations Office for Counter-Terrorism (UNOCT), Kompetenzzentrum Sicheres Österreich (KSÖ) und das Bundesministerium für Inneres (BMI), EU-Missionen sowie nationale Infrastrukturbetreiber wie Wien-IT oder Energienetzbetreiber wie z. B. Verbund, EVN und Salzburg AG. Außerdem kooperieren die Expert:innen auch beispielsweise über Initiativen der Wirtschaftskammer Österreichs (WKO) mit der Digital Factory Vorarlberg (DFV) sowie mit Unternehmen der herstellenden Industrie und KMU zusammen.

Entsprechend umgesetzte Trainings für die Entwicklung von besonderen Fähigkeiten für Behörden und Infrastrukturbetreiber erfolgten z. B. in Europa (Großbritannien, Slowenien, Rumänien und der Ukraine), in jenen Ländern Afrikas, in denen Französisch oder Englisch gesprochen wird, sowie in den arabischen Staaten Oman und den Vereinigten Arabischen Emiraten. Ebenso erfolgten Trainingstätigkeiten in asiatischen Ländern wie Korea, Thailand, den Philippinen und Vietnam sowie in Südamerika. Gemeinsam mit dem Außenministerium der Republik Österreich (BMEIA) war das AIT Center for Digital Safety & Security auch einer der Hauptakteure bei der Unterzeichnung der UN Cyber Crime Convention durch die Republik Österreich in Vietnam und die treibende Kraft für die Etablierung einer Kooperation zwischen Vietnam und Österreich auf dem Gebiet des Cyber Security Capacity Building.

AIT Cyber Range

Penetration Testing & Red Teaming

Der Penetrationstest, kurz Pentest, ist ein empirischer Sicherheitscheck, der unter definierten Rahmenbedingungen stattfindet. Dabei werden reale bzw. gängige Mittel und Techniken eingesetzt, die auch von potenziellen Angreifern verwendet werden. Penetrationstests zeigen eine Momentaufnahme der getesteten Komponenten aus einer bestimmten Perspektive. Generell erhöht sich die Anzahl der eruierten Schwachstellen mit dem eingesetzten Aufwand und den verfügbaren Informationen über das zu testende System.

Der Großteil der derzeit auf dem Markt angebotenen Penetrationstests konzentriert sich auf die Ausnutzung bereits bekannter Schwachstellen. In diesem Fall sind die Tester:innen, die durch die Sicherheitssoftware unterstützt werden, auf die automatisierte Evaluierung des Sicherheitslevels der Testkomponenten angewiesen. Die Expert:innen am AIT verfolgen hier einen anderen Ansatz. Die Spezialist:innen bringen ihre Expertise aus einer Vielzahl hochkarätiger Forschungsprojekte ein. Dadurch fördern die Tests auch neue, vorher unbekannte Schwachstellen (Zero-Day-Lücken) zu Tage. Das Team des Centers unterstützt Kund:innen vom ersten Prototypen bis zur finalen Implementierung. Ob Black-Box-Tests ohne genaue Kenntnis des zu testenden Systems oder White-Box-Tests, mit vollständiger Information bis hin zur umfangreichen Quellcode-Analyse. Die Expert:innen verfügen über das notwendige Know-how und langjährige Projekterfahrung.

IT Security ist ein hochsensibles Thema, daher werden keine Referenzen veröffentlicht. Betreute Kund:innen stammen aus allen Bereichen der Wirtschaft, der Kultur, den Medien, der Politik, dem Sport sowie dem öffentlichen Sektor. Um dennoch die Kompetenz auf diesem Gebiet zu unterstreichen, sind einige von den Expert:innen entdeckten und gemeldete Sicherheitslücken hier gelistet.

Security Advisories

Weitere Informationen über zertifizierte Serviceleistungen des AIT Center for Digital Safety & Security in den Bereichen Pentesting, Red and Purple Teaming und Schwachstellen-Scans/Security Audits sind hier zu finden.

Penetration Testing

Security Consulting

Das Center bietet seine breite Expertise aus dem Bereich Cyber Security auch als individuelle Beratungsdienstleistung an. Gemeinsam mit Kund:innen bestimmen die Expert:innen die individuelle Ausgangssituation und diskutieren die aktuellen Problembereiche und Anforderungen für die Zukunft. Im Vorfeld des Beratungsprojekts werden überschau- und bewältigbare Module mit klarer Ergebnisorientierung definiert, um den Kund:innen die Möglichkeit für eine selbständige und nachhaltige Weiterentwicklung im eigenen Unternehmen zu geben. Der dadurch erzielte Fortschritt auf Kundenseite stellt einen bedeutenden Schritt in Richtung cybersicherer Gesellschaft dar.

Die Security-Consulting-Services des AIT unterstützen Organisationen ganzheitlich dabei, ihre IT sicher, resilient und zukunftsfähig auszurichten. Das Angebot reicht von der Optimierung und Neugestaltung von IT- und Geschäftsprozessen, über den Aufbau wirksamer Informationssicherheits- und Business-Continuity-Managementsysteme bis hin zu strategischer IT-Ausrichtung. Ebenso zählen Audits nach anerkannten Standards sowie die praxisnahe Umsetzung von Datenschutzanforderungen dazu. Das Ziel ist es, Risiken zu minimieren, regulatorische Anforderungen effizient zu erfüllen und die IT als verlässliche Grundlage für stabile, nachhaltige Geschäftsprozesse zu etablieren.

Security Consulting

2 DATA SCIENCE & ARTIFICIAL INTELLIGENCE

Im Bereich Data Science & AI entwickelt im Center for Digital Safety & Security ein Team aus rund 50 Expert:innen menschenzentrierte, vertrauenswürdige und erklärbare KI-Lösungen, die gezielt gesellschaftliche, wirtschaftliche und sicherheitsrelevante Herausforderungen adressieren. Der Fokus liegt auf verantwortungsvoll gestalteter angewandter KI, die einen echten Mehrwert schafft. Beginnend bei datengetriebenen Entscheidungsgrundlagen für Behörden und Unternehmen, über den Schutz von Konsument:innen und demokratischen Entscheidungsprozessen bis hin zur Absicherung kritischer Infrastrukturen. Die KI-Systeme des AIT sind darauf ausgelegt, komplexe unstrukturierte Daten aus Bildern, Videos, Audio- und Textquellen sowie aus Sensordaten zu analysieren und Prognosen über zukünftige Entwicklungen abzuleiten.

Ein zentrales Element der Forschung ist die Erklärbarkeit und Nachvollziehbarkeit von KI-Entscheidungen, die als wesentlicher Erfolgsfaktor für Vertrauen, Akzeptanz und regulatorische Konformität gilt. Durch die enge Verbindung von Data Science, modernsten KI-Methoden und ethischen Leitprinzipien trägt das AIT Center dazu bei, die digitale Souveränität zu stärken und Innovationen nachhaltig, nachvollziehbar und gesellschaftlich wirksam umzusetzen.

Darüber hinaus verfolgt das Center konsequent einen Vertical-AI-Ansatz, bei dem eine tiefgehende Domänenexpertise mit modernsten KI-Methoden kombiniert wird. Das Ziel ist die Entwicklung maßgeschneiderter Lösungen für unterschiedliche Anwendungsfelder, von spezialisierten Fachanwendungen bis hin zu komplexen, sektorübergreifenden Systemen. Die Kompetenzen des Centers sind bewusst technologie- und branchenübergreifend angelegt, um vielfältige KI-Herausforderungen fundiert, verantwortungsvoll und praxisnah adressieren zu können.

Data Science & AI

Kampf gegen Desinformation

Die Expert:innen entwickeln Algorithmen und Technologien zur Analyse, Interpretation und verständlichen Aufbereitung multimedialer Inhalte wie Bilder, Videos, Audiodateien und Texte. Mithilfe moderner Computer-Vision-Methoden werden Objekte, Gesichter und Muster in Medieninhalten automatisch erkannt, klassifiziert und hinsichtlich ihrer Authentizität bewertet.

Ergänzend kommen Natural Language Processing (NLP) und Explainable AI (XAI) zum Einsatz, um textbasierte Inhalte wie Untertitel, Social-Media-Posts, Kommentare oder Metadaten zu analysieren sowie Aussagen über Plausibilität, Herkunft und mögliche Manipulationen zu treffen. Durch die Kombination visueller und sprachbasierter Analyseverfahren können multimodale Falschinformationen zuverlässig erkannt, nachvollziehbar erklärt und kontextualisiert werden.

Zusätzlich ermöglichen Verfahren zur Kontextanreicherung den Abgleich von Medieninhalten mit weiterführenden Informationen wie Ort, Zeit oder Quellen. Die modular und skalierbar ausgelegten Methoden erlauben die effiziente Verarbeitung großer Datenmengen und unterstützen Anwendungen in der digitalen Forensik, der Desinformationsbekämpfung, im OSINT (Open Source Intelligence)-Umfeld sowie bei sicherheitskritischen Analysen durch Strafverfolgungs- und Sicherheitsbehörden.

Media Intelligence

AIT Media Intelligence

AIT Media Intelligence Plattform

Die AIT Media Intelligence Plattform ist ein KI-gestütztes, modulares Analyse-Ökosystem für die forensische Untersuchung digitaler Medieninhalte. Sie unterstützt menschliche Expert:innen bei der Identifikation von Desinformation, Manipulationen und demokratiegefährdenden Inhalten und bietet Behörden, Organisationen und Unternehmen leistungsfähige Werkzeuge für Fact-Checking, Medienverifikation und Lagebildanalyse. Die Plattform kombiniert Digital Multi-Media Forensics, Context Enrichment und erklärbare KI (Explainable AI), um große Mengen an Text-, Bild-, Audio- und Videodaten effizient zu analysieren und in einen nachvollziehbaren Kontext zu setzen. Der modulare Aufbau erlaubt den gezielten Einsatz spezialisierter Analysewerkzeuge, die flexibel kombiniert und skalierbar betrieben werden können.

Zu den zentralen Funktionen zählen die Erkennung von Deepfake-Videos und -Sprache, synthetischen Gesichtern, Face-Morphing, KI-generierten Bildern sowie manipulierten Medieninhalten. Ergänzt wird dies durch Natural Language Processing zur Analyse von Hate Speech, Extremismus, Propaganda, Verschwörungstheorien, Diskriminierung und toxischer Sprache. Darüber hinaus unterstützt die Plattform die Wissensextraktion durch Text- und Sentiment-Analyse, Stil- und Schreibmustererkennung, Bild- und Video-Recherche, Objekt- und Symbolerkennung sowie Bild-Geolokalisierung.

Die AIT Media Intelligence Plattform liefert Echtzeitergebnisse, unterstützt kollaboratives Arbeiten und ist als kontinuierlich weiterentwickelte Lösung sowohl online als auch über maßgeschneiderte Implementierungen sowie Integrationen verfügbar. Damit ermöglicht diese das Erkennen, Verstehen und das Kontextualisieren komplexer medialer Inhalte im Sinne einer Grundlage für fundierte Entscheidungen in sicherheits-, gesellschafts- und demokratierelevanten Anwendungsfeldern.

Media Intelligence

DisDETECT – Plattform zur Erkennung und Analyse von Desinformation

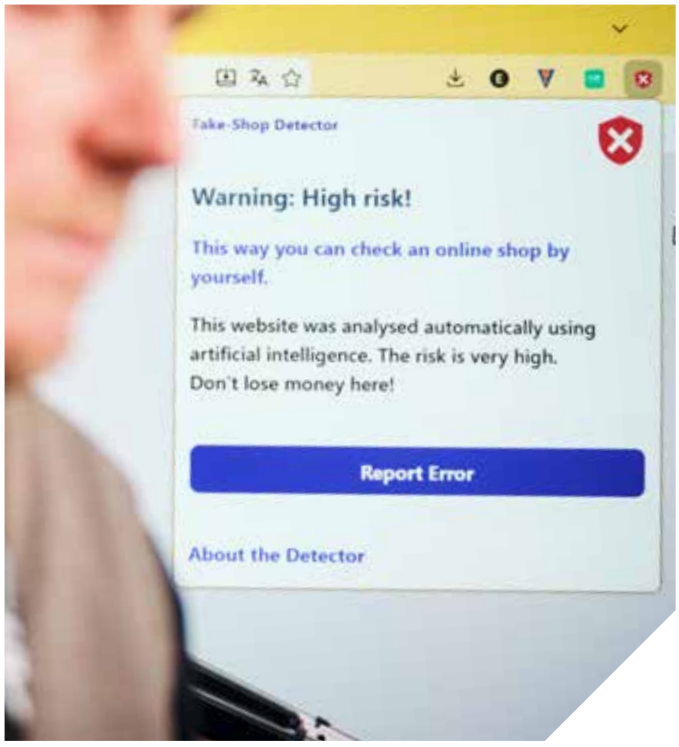
DisDETECT ist ein System zur semi-automatischen Erkennung und Analyse von Desinformation sowie verwandten Phänomenen wie Hate Speech, toxischer Sprache und Propaganda in deutschsprachigen Online-Medien. Es kombiniert narrative, argumentative und framing-bezogene Merkmale mit Transformer-Modellen, linguistischen Features und Wissensgraph-Einbettungen, um unterschiedliche Kommunikationsformen zuverlässig zu erfassen. Die Ergebnisse werden in einer webbasierten Anwendung mit interaktiven Visualisierungen als Grundlage für eine anschließende Analyse von Expert:innen dargestellt.

Fake-Shop Detector

Fake-Shop Detector

Fake-Shops im Internet werden zahlreicher und zugleich schwieriger zu erkennen. Eine Unterstützung beim Aufspüren der Onlinebetrüger bietet der Fake-Shop Detector, eine Entwicklung des AIT Centers in enger Kooperation mit dem Österreichischen Institut für angewandte Telekommunikation (ÖIAT) sowie dem österreichischen IT-Spezialisten X-Net. Der Fake-Shop Detector überprüft unbekannte Online-Shops mithilfe Künstlicher Intelligenz in Echtzeit auf mehr als 21.000 Merkmale. Dabei ist vor allem eine permanente Qualitätskontrolle der Künstlichen Intelligenz durch den Menschen inhärenter Teil der KI-basierten Lösung.

Ist ein Shop verdächtig, warnt der Detector und schützt Konsument:innen präventiv vor Online-Betrug. Der Erfolg des Fake-Shop Detectors mündete in eine Partnerschaft zwischen AIT und dem bayrischen Justizministerium. Deren Ziel ist es, den Detector auf die besonderen Anforderungen der Strafverfolgungsbehörden abzustimmen und für deren Ermittlungsarbeit weiterzuentwickeln. Darüber hinaus wurde dieses Tool mehrfach preisgekrönt (eAward 2023, Staatspreis Digitalisierung 2024, Constantinus Award 2024, KSÖ-Sicherheitspreis 2024) und war zuletzt österreichischer Gewinner unter 35 internationalen Cybersicherheitsprodukten, die vom unabhängigen Systemtestexperten „AV-Comparatives“ auf ihre Wirksamkeit gegen Fake-Shops getestet wurden. Die Entwicklung des Fake-Shop Detectors wurde durch Mittel des Österreichischen Bundesministeriums für Finanzen im KIRAS Sicherheitsforschungsprogramm finanziert.



Knowledge Management

Im Bereich Knowledge Management entwickelt das AIT Center Methoden zur effizienten Erschließung und Nutzung großer, heterogener Datenbestände. Die Arbeiten basieren auf mehr als zwei Jahrzehnten Forschung zur Bereitstellung des Zugangs zu digitalen Kulturgütern auf Grundlage der sogenannten FAIR-Prinzipien (Findable, Accessible, Interoperable, Reusable), unter anderem in Zusammenarbeit mit dem europäischen Kulturerbe-Portal Europeana.

Der Fokus liegt auf der multimodalen Informationsgewinnung, bei der unterschiedliche Datenformen – etwa Text, Bild oder strukturierte Daten – gemeinsam analysiert und miteinander verknüpft werden. Durch crossmodale Suchverfahren (z. B. Text-zu-Bild oder Bild-zu-Text) sowie nutzerfreundliche Ergebnisdarstellungen können relevante Informationen in großen Datenbeständen effizient gefunden und in kuratierten Datensammlungen aufbereitet werden.

Zum Einsatz kommen semantische und einbettungsbasierte Indizierungsmethoden sowie Large Language Models, die natürliche Sprachabfragen über heterogene Datenquellen ermöglichen. Das Ziel ist es, bestehende Informationsbestände in reichhaltige semantische Strukturen wie etwa Wissensgraphen zu überführen und so ihre Nutzung für Analyse und Forschung sowie Entscheidungsprozesse nachhaltig zu verbessern.

Europeana

Knowledge Management

3 DIGITALES IDENTITÄTSMANAGEMENT

Das AIT Center for Digital Safety & Security entwickelt modernste Technologien zur raschen, präzisen und sicheren Erkennung sowie Verifikation von Identitäten. Diese Innovationen setzen neue Maßstäbe in Sicherheit, Komfort und Datenschutz. Sie sind ein internationales Erfolgsbeispiel für die verantwortungsvolle Digitalisierung sicherheitskritischer Anwendungen. Die Grundlage dafür bildet das nationale Sicherheitsforschungsprogramm KIRAS des Bundesministeriums für Finanzen (BMF), in enger Zusammenarbeit mit dem Bundeministerium für Inneres (BMI) als Bedarfsträger und internationalem Vorreiter im Sicherheitsbereich. Gemeinsam mit der technologischen Forschungs- und Entwicklungsexzellenz des AIT positioniert dieses Zusammenspiel Österreich als internationales Vorzeigemodell für verantwortungsvolle Digitalisierung sensibler Daten und leistet damit einen entscheidenden Beitrag zur digitalen Souveränität Europas.

Mit der zunehmenden Digitalisierung von Dienstleistungen und der wachsenden Bedeutung sicherer Authentifizierungsverfahren steigt der Bedarf an innovativen, zuverlässigen und benutzerfreundlichen Technologien für digitale Identitäten und biometrische Sicherheitssysteme. Traditionelle biometrische Systeme wie kontaktbasierte Fingerabdrucksensoren in sicherheitskritischen Bereichen wie Flughäfen, stoßen zunehmend an ihre Grenzen. Kontaktbasierte Systeme sind anfällig für Manipulationen, unhygienisch und oft nicht benutzerfreundlich. Parallel dazu gewinnen automatisierte, vertrauenswürdige Videoanalyse- und Sensorsysteme in unterschiedlichen optischen Spektren an Bedeutung wie etwa für den Schutz kritischer Infrastrukturen, öffentlicher Räume oder strategischer Einrichtungen.

Gleichzeitig wächst das Bedürfnis nach verantwortungsvoll gestalteten, sicheren und datenschutzkonformen Lösungen, die sowohl den Anforderungen der Nutzer:innen als auch den strengen Sicherheitsvorgaben entsprechen. Die EU verfolgt im Rahmen ihrer digitalen Souveränitätsstrategie das Ziel, solche Technologien unabhängig und sicher innerhalb ihres Geltungsbereichs zu entwickeln und einzusetzen. Auch Organisationen wie die Vereinten Nationen (UN) unterstützen die globale Staatengemeinde bezüglich der Etablierung sicherer Systemlösungen und eines verantwortungsvollen Umgangs mit sensitiven biometrischen Daten.

Computer Vision

Biometrische Sensorlösungen

Im Bereich von Technologien für die Verifikation von digitalen Identitäten und moderner biometrischer Sensorik gilt das AIT mit dem Center for Digital Safety & Security als ein wichtiger internationaler Technologieführer für kontaktlose und somit sichere, hygienische und benutzerfreundliche Fingerprint-Sensorik im Sinne einer biometrischen Authentifizierung.

Die Institution leistet damit einen wichtigen Beitrag zur digitalen Souveränität der EU ebenso wie in der globalen Sicherheitsinfrastruktur. Durch diese Technologieentwicklung „Made in Austria" leistet das AIT heute einen wichtigen Beitrag zu den digitalen Souveränitätszielen der EU.

Die Führungsrolle des AIT im Bereich kontaktloser Fingerprint-Sensorik wird durch internationale Lizenzvereinbarungen mit Anbietern wie T3K und einem globalen Flughafensicherheitsunternehmen, einer Zertifizierungskooperation mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie durch die Zusammenarbeit mit dem UN Office for Counter-Terrorism (UNOCT) auf der Plattform www.responsible-biometrics.org eindrucksvoll dargestellt.

Responsible Biometrics

Zusätzlich laufen bereits konkrete Technologieeinführungsprojekte mit Industriepartnern und Behörden innerhalb der EU im Sinne einer mit Verantwortung geführten Einführungsphase, wie etwa der Rollout der neuen Fingerprint-Sensorik bei der österreichischen Polizei. Ebenso ist bei diesen digitalen Zukunftstechnologien eine Kooperation mit den UN im globalen Kontext geplant.

Face-Snap – mobile Erfassung biometrischer Gesichtsprofile

Im Kontext digitaler Identitätslösungen entwickelt das Center for Digital Safety & Security innovative Anwendungen für die mobile biometrische Erfassung. Face-Snap ermöglicht die schnelle und sichere Erstellung von Gesichtsprofilen direkt über ein Smartphone und unterstützt damit die Einsatzkräfte bei der effizienten Durchführung ihrer täglichen Arbeit. Die Anwendung erlaubt es, hochwertige Gesichtsaufnahmen direkt im Einsatzfeld zu erfassen und unmittelbar weiterzuverarbeiten. Dadurch wird das bislang aufwendige Verfahren der Gesichtserfassung deutlich vereinfacht, was Zeit spart und die Effizienz von Ermittlungs- und Identifizierungsprozessen verbessert. Face-Snap integriert außerdem automatisierte Qualitätsprüfungen auf Basis internationaler ICAO-Standards. Die Anwendung gibt Nutzer:innen Hinweise, wenn Aufnahmen optimiert werden sollten, um die bestmögliche Bildqualität sicherzustellen. Das gewährleistet, dass nur geeignete und standardkonforme Bilder in biometrische Datenbanken aufgenommen werden. Die Entwicklung der Lösung erfolgte in enger Zusammenarbeit mit Polizeibehörden, um sicherzustellen, dass rechtliche, operative und sicherheitsrelevante Anforderungen von Beginn an berücksichtigt werden. Face-Snap unterstützt Behörden dabei, ihre Verfahren effizienter zu gestalten und gleichzeitig hohe Anforderungen an den Datenschutz und die Sicherheit erfüllen zu können. Face-Snap ist ein wichtiger Baustein moderner digitaler Identitätslösungen im Sicherheitsbereich.

Touchless Four Fingerprint (T4F) Scanner

T4F

Der Touchless Four Fingerprint (T4F) Scanner ermöglicht mittels kamerabasierter Aufnahme die kontaktlose Erfassung von vier Fingerabdrücken gleichzeitig. Diese Lösung stellt höchste Anforderungen an Hygiene, Sicherheit sowie Nutzerkomfort und eignet sich insbesondere für Zugangskontrollen, Grenzkontrollen und sichere Authentifizierungsprozesse. Durch die berührungslose Erfassung werden latente Fingerabdrücke vermieden, Täuschungsversuche erschwert und gleichzeitig eine kompatible Nutzung bestehender Fingerabdruckdatenbanken ohne Anpassungen an nachgelagerte Verifikations- oder Authentifizierungssysteme sichergestellt.

Biometrische Sensorik

4 SCHUTZ KRITISCHER INFRASTRUKTUREN

Moderne Gesellschaften sind auf leistungsfähige und sichere Infrastrukturen angewiesen. Gleichzeitig steigen die Anforderungen an deren Verfügbarkeit, Resilienz und Schutz. Betreiber kritischer Infrastrukturen benötigen daher neue Ansätze, um den Zustand ihrer Systeme kontinuierlich zu überwachen, potenzielle Störungen frühzeitig zu erkennen und Risiken gezielt zu minimieren. Das AIT entwickelt hierfür intelligente Monitoring- und Analyseverfahren. Dazu kombinieren die Expert:innen moderne Sensortechnologien, datengetriebene Analysen und operative Entscheidungsunterstützung. So wird Transparenz über den Zustand von Anlagen und Netzen geschaffen und resiliente Betriebsprozesse ermöglicht.

Ein zentraler Kompetenzbereich ist Distributed Acoustic Sensing (DAS). Dabei werden bestehende Glasfaserinfrastrukturen als großflächige, kontinuierliche Sensornetzwerke genutzt. So können Ereignisse entlang der Infrastrukturen detektiert und analysiert werden. Ergänzend dazu stärkt das AIT den Schutz kritischer Infrastrukturen durch optische Sensorik und Videoanalyse in unterschiedlichen Spektralbereichen. Die entwickelten Technologien unterstützen Akteure der öffentlichen Sicherheit bei der automatisierten, vertrauenswürdigen und benutzerfreundlichen Auswertung visueller Informationen. Durch die Verbindung von verteilter akustischer und optischer Sensorik, KI-gestützter Interpretation sowie operativer Informationsaufbereitung schafft das AIT Lösungen, die Sicherheitsorganisationen, Infrastrukturbetreiber und öffentliche Stellen dabei unterstützen, kritische Situationen früher zu erkennen, komplexe Umgebungen besser zu verstehen und koordinierter zu handeln.

Critical Infrastructure Protection

fiberRAIL® – Distributed Acoustic Sensing (DAS)

fiberRAIL®

Kritische Infrastrukturen wie Eisenbahnnetze, Straßen, Energie- und Kommunikationsleitungen erstrecken sich über große Distanzen und müssen kontinuierlich überwacht werden. Klassische Überwachungslösungen basieren auf punktuellen Sensoren oder Kameras, die nur begrenzte Bereiche abdecken, hohe Installations- und Wartungskosten verursachen und sich nur schwer skalieren lassen. Gleichzeitig steigen die Anforderungen an Sicherheit, Verfügbarkeit und Effizienz – insbesondere im Verkehr und bei sicherheitskritischen Anlagen. Distributed Acoustic Sensing (DAS) bietet grundsätzlich die Möglichkeit, diese Lücke zu schließen. DAS kann beispielsweise eine ideale Ergänzung für die Positionsbestimmung von Zügen bieten, da es – anders als Global Navigation Satellite System (GNSS) – infrastrukturseitig unter der vollen Kontrolle des Bahninfrastrukturbetreibers steht, Positionen in Echtzeit mit hoher Genauigkeit ermitteln kann und gleichzeitig auch den Zuganfang und das Zugende lokalisiert.

Das AIT Center nimmt eine führende Rolle an der Schnittstelle von DAS-Technologie, KI-basierter Analyse und sicherheitskritischen Anwendungen ein. fiberRAIL® ist ein am AIT entwickeltes innovatives, optisch-faserbasiertes Track-&-Monitor-System, das Bahninfrastrukturbetreiber dabei unterstützt, Züge und Gleisanlagen in Echtzeit zu überwachen, ganz ohne zusätzliche Hardware an Fahrzeugen oder teurer Sensorik im Gleis. Durch Nutzung bestehender Glasfaserkabel entlang der Strecke liefert die Lösung kontinuierliche Informationen zu Zugposition, Geschwindigkeit, Länge sowie Bewegungsrichtung und ermöglicht eine präzise, lückenlose Lokalisierung aller Zugbewegungen.

Gleichzeitig erkennt fiberRAIL® sicherheitskritische Ereignisse wie Schienenbrüche, Radschäden, Entgleisungen oder verlorene Wagen frühzeitig und meldet alle Vorfälle in Echtzeit. Die Plattform unterstützt darüber hinaus vorausschauende Wartung (Predictive Maintenance) und die Sicherheit von Arbeitskräften auf der Strecke. Gleichzeitig wird eine Dokumentation über die Steuerung und damit das Fahrverhalten zur Verschleißminimierung der Infrastruktur angelegt. fiberRAIL® ist modular, wartungsarm und erhöht sowohl Sicherheit als auch Effizienz im Bahnbetrieb.

FrontierSense

Optische Sensorik – FrontierSense

Der AIT Forschungsschwerpunkt im Bereich der optischen Sensorik stärkt die wichtigsten industriellen und staatlichen Interessengruppen im Bereich der öffentlichen Sicherheit durch die Bereitstellung unterstützender videoanalytischer Technologien. Die Expert:innen des Centers arbeiten an vertrauenswürdigen, automatisierten und benutzerfreundlichen sowie innovativen Lösungen, die zur Videoanalyse in verschiedenen optischen Spektren beispielsweise an Grenzübergängen an Land und auf See eingesetzt werden können. Die Zielgruppe sind Akteure rund um den Schutz kritischer Infrastrukturen (Grenzen, Kraftwerke, Verkehrsknotenpunkte, etc.), öffentlicher Bereiche (Veranstaltungsgelände, Festivals, etc.) ebenso wie entlegener Gebiete (z. B. Ölfelder) oder im Verteidigungsbereich.

Mit FrontierSense wurde eine schnell einsatzbereite Multisensorplattform mit Edge-KI geschaffen, die als kompakte, modulare Lösung konzipiert wurde und in operativen Grenzgebieten eine Echtzeit-Lageerfassung ermöglicht. Die Plattform wurde für kritische und ressourcenbeschränkte Umgebungen entwickelt und integriert heterogene Sensoren mit bewährten, gerätebasierten KI-Analysen. So können Objekte, Ereignisse oder Umgebungen in Echtzeit automatisch erkannt, interpretiert und kontextualisiert werden. FrontierSense bietet Entscheidungsunterstützung genau dort, wo sie am dringendsten benötigt wird. Die vielfältigen, heterogenen Sensoren liefern robuste, analysefertige Daten, die auch bei widrigen Wetterbedingungen und in komplexen Umgebungen interpretierbar und zuverlässig bleiben.

Aufbauend auf einer interoperablen und modularen Architektur kombiniert FrontierSense eine robuste Multisensor-Datenerfassung (FrontierSense Core) mit fortschrittlicher, Edge-basierter Künstlicher Intelligenz und Analytik (FrontierSense Insight). Dadurch ermöglicht die Plattform einen skalierbaren Einsatz in sicherheitsrelevanten Bereichen und kritischen Infrastrukturen. Durch die lokale Datenverarbeitung am Edge reduziert FrontierSense Latenzzeiten, wahrt die Datenhoheit und gewährleistet einen ausfallsicheren Betrieb auch bei eingeschränkter Konnektivität.

FrontierSense liefert Betreibern und Behörden zeitnahe und umsetzbare Erkenntnisse, verbessert das Situationsbewusstsein, unterstützt fundierte Entscheidungen und stärkt die operative Ausfallsicherheit an jeder Grenze.

Optische Sensorik

5 KRISEN- UND KATASTROPHENMANAGEMENT

In dynamischen und sicherheitskritischen Umgebungen ist ein aktuelles und verlässliches Lagebild entscheidend, um effektiv zu koordinieren und fundierte Entscheidungen zu treffen. Behörden, Einsatzorganisationen und Betreiber kritischer Infrastrukturen müssen Informationen aus unterschiedlichsten Quellen zusammenführen, bewerten und in kurzer Zeit in konkrete Maßnahmen überführen. Das AIT entwickelt daher Systeme zur Lagebeurteilung und Entscheidungsunterstützung. Diese verbinden heterogene Datenquellen, Sensorinformationen, Geodaten und operative Prozesse zu einem gemeinsamen Lagebild. Dadurch unterstützen die AIT-Expert:innen Organisationen dabei, komplexe Situationen besser zu verstehen, Risiken frühzeitig zu erkennen und koordinierte Entscheidungen in Echtzeit zu treffen.

Mit seinen Lösungen trägt das AIT dazu bei, die Krisenreaktion, das Katastrophenmanagement und die gesellschaftliche Resilienz nachhaltig zu verbessern. Das Ziel ist es, Einsatzorganisationen und öffentliche Stellen mit vertrauenswürdigen, praxistauglichen und technologisch fortschrittlichen Systemen zu unterstützen.

Krisen- & Katastrophen-management

Lagebild & CBRNe

Die Bereitstellung optimierter Entscheidungsgrundlagen ist eine zentrale Anforderung für das Krisen- und Katastrophenmanagement. Der Fokus liegt auf digitalen Plattformen und Systemlösungen, die eine interoperable und sichere Kommunikation, gemeinsame Lagebilder sowie eine koordinierte Entscheidungsfindung zwischen Einsatzkräften, Behörden und Betreibern kritischer Infrastrukturen ermöglichen.

In einer zunehmend komplexen globalen Sicherheitslandschaft ist die Fähigkeit, chemische, biologische, radiologische nukleare und explosive (CBRNe) Bedrohungen zu erkennen und darauf zu reagieren, wichtiger denn je. Fortschritte in der Überwachungstechnologie und bei Systemen zur Lagebilderkennung prägen die Zukunft der Verteidigung sowie der Notfallhilfe. Sie ermöglichen eine schnellere, präzisere Identifizierung und Bewältigung von Bedrohungen. Durch die Kombination von Spitzenforschung und internationaler Zusammenarbeit entstehen innovative Lösungen zur Verbesserung der Sicherheit für Streitkräfte und Katastrophenschutzbehörden, aber auch für die Bevölkerung. Vor diesem Hintergrund weist auch der CBRNe-Aktionsplan der Europäischen Kommission darauf hin, dass die EU ihre Widerstandsfähigkeit stärken und ihre Vorsorge für den Umgang mit CBRNe-Bedrohungen verbessern muss.

In den vergangenen 15 Jahren konnte das AIT Center for Digital Safety & Security in vielen Projekten der österreichischen Sicherheitsforschungsprogramme (KIRAS und Forte) sowie von europäischen Sicherheitsforschungsprogrammen (FP7, H2020, Horizon Europe) eine umfassende Expertise im Bereich von Sensortechnologien für die Lagebilderstellung und Situationsanalyse aufbauen. Mit dem Know-how, das bei der Entwicklung des CBRNe-Risikobewusstseins und dem Schutz ziviler sowie militärischer Kräfte in Krisen- und Notfallsituationen gewonnen wurde, übernahm das AIT auch eine führende Rolle in Initiativen europäischer Verteidigungsprogramme.

Ein zentraler Bestandteil der digitalen CBRNe-Verteidigung ist die Entwicklung modularer System-of-Systems-Architekturen, die Sensoren, Plattformen und Softwarekomponenten zu einem integrierten Gesamtsystem verbinden. In diesem Zusammenhang wurden neue funktionale Softwarekomponenten für die Situational Awareness entwickelt sowie ein multinationales Integrationskonzept für CBRNe-Aufklärungs- und Überwachungssysteme definiert. Diese Architektur schafft die Grundlage für eine flexible Integration bestehender und zukünftiger Technologien.

Im Bereich der Entscheidungsunterstützung im Krisen- und Katastrophenmanagement entwickelte das Center Methoden zur optimierten Auswahl und zur objektiven Bewertung von Lösungen sowie zur Validierung der Auswirkungen von Maßnahmen. Für eine verbesserte Kooperation der Akteure wird außerdem der Einsatz von Datenräumen im Krisen- und Katastrophenmanagement vorangetrieben. Anwendungsfälle sind mit dem Ressourcenmanagement verbunden, das einen verbesserten, organisationsübergreifenden Einsatz von Freiwilligen ermöglicht, sowie resiliente Lieferketten in Krisensituationen sicherstellt.

Lagebild

Softwareplattform Horus3D

Die Softwareplattform Horus3D bildet eine wesentliche technologische Komponente für die Analyse komplexer Umgebungen. Sie verarbeitet Sensordaten unterschiedlicher Plattformen und erzeugt daraus detaillierte dreidimensionale Modelle des Geländes sowie der Infrastruktur. Diese digitalen Modelle ermöglichen automatisierte Umgebungsanalysen und unterstützen Einsatzkräfte bei der operativen und taktischen Planung. Gleichzeitig dienen sie als Grundlage für digitale Zwillinge von Einsatzumgebungen.

Neben luftgestützten Systemen wurde Horus3D auch für robotergestützte Inspektionssysteme erweitert, die in komplexen Innenräumen oder gefährlichen Umgebungen eingesetzt werden können. Durch die Erstellung digitaler Zwillinge lassen sich Roboterplattformen aus der Ferne steuern, während gleichzeitig automatisierte 3D-Analysen der Umgebung durchführbar sind. Diese unterstützen Spezialist:innen bei der Analyse verdächtiger Objekte, der Detektion von CBRNe-Substanzen sowie bei der Überwachung kritischer Infrastruktur.

Software-Framework MuFASA

Eine weitere Schlüsseltechnologie ist die Multimodal Fusion Architecture for Sensor Applications (MuFASA). Dieses Software-Framework ermöglicht die intelligente Fusion von Daten aus unterschiedlichen Sensorquellen auf Feature-Ebene. Durch die Kombination räumlich und zeitlich korrelierter Sensordaten lassen sich Fehlalarme reduzieren und die Zuverlässigkeit von Alarmmeldungen deutlich erhöhen. Gleichzeitig erlaubt die modulare Struktur eine Erweiterung auf neue Sensorarten und Anwendungsfelder.

Die Kombination dieser Technologien schafft eine leistungsfähige digitale Infrastruktur für moderne CBRNe-Situational-Awareness-Systeme. Durch die Integration von Sensorik, automatisierter Datenanalyse und 3D-Umgebungsmodellen entsteht ein umfassendes Lagebild, das Einsatzorganisationen dabei unterstützt, Gefahren frühzeitig zu erkennen und fundierte Entscheidungen zu treffen.

Im Bereich Krisen- und Katastrophenmanagement besitzt das AIT vor diesem Hintergrund gegenwärtig einen ausgezeichneten Ruf als international anerkanntes Kompetenzzentrum. Derzeit liegt der Schwerpunkt auf den CBRNe-Komponenten Detection Identification Monitoring (DIM) und Knowledge Management (KM). Es ist geplant, Hazard Management (HM) und Physical Protection (PP) in zukünftigen europäischen Projekten zu adressieren und damit das „System of Systems" zu erweitern.

Software-Modul RaptoR

Für die radiologische Lageerkundung wurde das Software-Modul RaptoR entwickelt, das eine präzise Kartierung radioaktiver Belastungen mithilfe unbemannter Luftfahrzeuge ermöglicht. Während des Fluges erfassen Sensoren radiologische Messdaten, die zur Lokalisierung mehrerer radioaktiver Quellen sowie zur Erstellung von Dosisleistungskarten genutzt werden.

In Kombination mit der 3D-Analyse können auch schwer zugängliche Bereiche präzise erfasst werden. Darüber hinaus ermöglicht die Technologie die Detektion chemischer Substanzen und die Analyse von Geländestrukturen zur Unterstützung automatisierter Probeentnahmen.kritischer Infrastruktur.

6 SUSTAINABLE & RESILIENT SOCIETY

Für eine nachhaltige und resiliente Gestaltung von Städten, Regionen und Infrastrukturen sind zunehmend datenbasierte Entscheidungen und eine enge Zusammenarbeit zwischen öffentlichen Einrichtungen, Infrastrukturbetreibern, Unternehmen und Bürger:innen erforderlich. Gleichzeitig werden Umwelt-, Klima- und Nachhaltigkeitsfragen immer komplexer und erfordern integrierte Lösungen, die Informationen aus unterschiedlichen Quellen zusammenführen und in operative Prozesse einbinden.

Das AIT entwickelt digitale Lösungen, die das Nachhaltigkeitsmanagement, die Klimaresilienz, das Umweltmonitoring und die digitale Transformation von Verwaltungs- und Infrastrukturprozessen unterstützen. Durch die Verbindung von Daten, Wissen und Entscheidungsunterstützung schaffen die AIT-Expert:innen die Grundlage für eine transparente, effiziente und vertrauenswürdige Zusammenarbeit in komplexen Ökosystemen. Die Anwendungsfelder reichen von Klimawandelanpassung und Luft- sowie Wasserqualitätsmonitoring über nachhaltige Land- und Forstwirtschaft bis hin zu erneuerbaren Energien, Kreislaufwirtschaft und evidenzbasierter Umweltpolitik.

Eine zentrale Voraussetzung für wirksames Handeln ist ein belastbares Verständnis der aktuellen Lage. Ob auf nationaler Ebene, in Regionen, Städten oder spezifischen Einsatzumgebungen: Umwelt- und Klimadaten müssen kontinuierlich erfasst, integriert und interpretiert werden, um Risiken, Belastungen und Entwicklungstrends sichtbar zu machen. Dies betrifft beispielsweise das Monitoring von Schadstoffen in Luft und Wasser, die Bewertung von Klimaanpassungsmaßnahmen oder die Modellierung zukünftiger Entwicklungen unter unterschiedlichen Rahmenbedingungen. Durch die Verbindung von Sensordaten, Umweltmodellierung, vertrauenswürdiger KI und entscheidungsorientierter Analyse schafft das AIT eine fundierte Grundlage für nachhaltiges und resilientes Handeln.

Sustainable & Resilient Society

Digitale Lösungen zum Schutz der Umwelt

Im Bereich Environmental Analytics werden zentrale Herausforderungen in den Bereichen Klima, Umwelt und Nachhaltigkeit adressiert. Das AIT Center entwickelt dafür datenbasierte Analysemethoden, die zur Umsetzung der Ziele des europäischen Green Deal beitragen. Im Fokus stehen Datenfusion, physikalisch informiertes maschinelles Lernen sowie erklärbare und vertrauenswürdige Prognosemodelle. Die Anwendungsfelder reichen von Klimawandelanpassung über nachhaltige Land- und Forstwirtschaft bis hin zu erneuerbaren Energien und Kreislaufwirtschaft.

Egal, ob global oder in spezifischen Umgebungen, wenn es um Umwelt und Klima geht, ist es zuallererst nötig, die aktuelle Situation zu verstehen, um darauf aufbauend verschiedene Handlungsoptionen bewerten zu können. Dies betrifft sowohl das laufende Monitoring von Schadstoffen in der Luft oder im Wasser als auch die Beurteilung bzw. das Monitoring von Maßnahmen sowie die Modellierung von zukünftigen Entwicklungen.

Mit den am AIT entwickelten Lösungen werden Länder, Entscheidungsträger:innen und Organisationen bei der Analyse der aktuellen Situation und der Planung künftiger Investitionen unterstützt. Aufbauend auf der gemeinsam mit dem Unternehmen ADES entwickelten Plattform AIRDB für den Betrieb großer Sensornetze, werden Lösungen zur Überwachung einer Vielzahl an Umweltparametern angeboten. Zur Erhebung von Emissionsquellen als Basis für die Erstellung von Szenarienmodellen wurde am AIT ergänzend die Plattform EMIKAT entwickelt. Damit können beispielsweise regulative Maßnahmen zur Klimaanpassung modelliert und objektiv bewertet werden.

Cooperative Digital Solutions

EMIKAT

EMIKAT – Komplettlösung zur Verwaltung und Analyse von Emissionsdaten

EMIKAT ist ein hochwertiges Datenmanagement- und Datenanalysesystem, das detaillierte Emissions- und Energieinventare liefert und eine fundierte Entscheidungsfindung zur Verminderung der Freisetzung von Luftschadstoffen ermöglicht.

Das System kann zur Berechnung und Visualisierung der Umweltauswirkungen aktueller und zukünftiger „Wenn-Dann-Szenarien" eingesetzt werden. Damit können beispielsweise wichtige Zukunftsthemen für die Stadtplanung, wie die Auswirkungen der Klimaerwärmung oder Maßnahmen zur Dekarbonisierung, simuliert werden.

Es liefert ein zeitlich und räumlich aufgelöstes Bild des Energieverbrauchs der Endverbraucher sowie der Luftschadstoff- und Treibhausgasemissionen. Damit ermöglicht das System die Analyse von Energieverbrauch und Schadstoffemissionen für verschiedene räumliche Einheiten und unterschiedliche Zeiträume.

AIRDB

AIRDB – Intelligente Lösung zur Luftqualitätsmessung

AIRDB ist eine performante und hoch präzise Sensornetzwerklösung zum Management und Monitoring großer Sensornetzwerke, beispielsweise im Bereich Luft oder Wasser. AIRDB, als robustes aber zugleich flexibles System, schafft als einzige Lösung den Spagat zwischen einer stationären zertifizierten „Fit for purpose"-Lösung und einer modernen Toolbox, die auch offen ist für andere Branchen, andere Messhardware und die Integration von Flächendaten.

Als flexible, moderne Plattform für Expert:innen und Organisationen im Umweltbereich deckt die moderne Architektur des Systems alle aktuellen Anforderungen an Regulatorien und Compliance aus fachlicher und IT-technischer Sicht ab. Messdaten können unabhängig von verwendeten Messstationsrechnern oder Erfassungsgeräten aufgenommen und einem revisionssicheren Verarbeitungsprozess zugeführt werden.

Expertenfunktionen stehen über moderne Browserapplikationen zur Verfügung und sind über Rollen und Rechte personalisiert auslieferbar. Datenbankzugriffe, Topologie- und Geräteverwaltung stehen ebenso wie Funktionsaufrufe komplexer Daten-Aggregationen (TimeSeriesEngine mit FORMULA© Expressions) für eine abgesicherte Integration in Drittsysteme via API zur Verfügung.

Smarte Städte & Kommunen

Städte und Gemeinden benötigen heute konkrete digitale Werkzeuge, um Entscheidungen in den Bereichen Klimaanpassung, nachhaltige Stadtentwicklung, Infrastrukturplanung und Krisenvorsorge fundiert treffen zu können. Das AIT Center for Digital Safety & Security entwickelt dafür praxisnahe Lösungen, die Daten aus unterschiedlichen Quellen integrieren, komplexe Informationen verständlich aufbereiten und daraus direkt nutzbare Entscheidungsgrundlagen ableiten. Die entwickelten Systeme werden bereits in europäischen Projekten und Pilotregionen eingesetzt und unterstützen Städte dabei, fragmentierte Datenlandschaften zu verbinden und strategische Maßnahmen transparent zu planen.

Datenaustausch

Eine zentrale Lösung ist die Entwicklung und Implementierung kommunaler Data Spaces, die einen sicheren und souveränen Datenaustausch zwischen Verwaltung, Infrastrukturbetreibern, Unternehmen und Forschungseinrichtungen ermöglichen. Die vom Center entwickelten Architekturen integrieren Daten aus Bereichen wie Umweltmonitoring, Energie, Mobilität, Gebäude und Klimarisiken in eine gemeinsame digitale Infrastruktur.

Diese Plattformen ermöglichen es Städten, bislang getrennte Datenquellen zusammenzuführen und für Planungs- und Entscheidungsprozesse nutzbar zu machen. In mehreren europäischen Projekten wurden entsprechende Datenraum-Konzepte bereits umgesetzt, beispielsweise für urbane Datenräume oder sektorübergreifende industrielle Anwendungen. Die entwickelten Governance-Modelle stellen sicher, dass Datenhoheit, Zugriffskontrolle und Interoperabilität gewährleistet sind, bei gleichzeitig langfristiger Nutzung der Systeme.

Wissensmanagement

Zur Unterstützung komplexer Entscheidungsprozesse entwickeln die Expert:innen des Centers KI-gestützte Wissensplattformen, die große Mengen an Dokumenten, Richtlinien, wissenschaftlichen Erkenntnissen und operativen Daten automatisch erschließen sowie miteinander verknüpfen. Die Systeme basieren auf semantischen Modellen und Wissensgraphen und ermöglichen eine strukturierte Navigation durch umfangreiche Informationsbestände.

In Forschungsprojekten wie NEB Junction, MAIA und AI4Health werden diese Technologien bereits eingesetzt, um Informationen aus unterschiedlichen Forschungs- und Praxisprojekten zusammenzuführen und für Nutzer:innen zugänglich zu machen. Ein konkretes Ergebnis ist der NEB Knowledge Hub, der Wissen aus verschiedenen New European Bauhaus Initiativen strukturiert verknüpft und wiederverwendbar macht.

MAIA

New European-Bauhaus

Kommunale Entscheidungsträger können damit relevante Informationen schneller finden, Zusammenhänge besser verstehen und ihre Maßnahmen an bestehenden Best Practices ausrichten.

Marktplatz

Das AIT Center entwickelt gemeinsam mit Partnern digitale Plattformen, die als Marktplatz für Daten, Modelle und Analysewerkzeuge dienen. Diese Plattformen integrieren Szenarioanalyse, Planungswerkzeuge und Datenquellen in eine gemeinsame digitale Umgebung und ermöglichen Städten, unterschiedliche Entwicklungsoptionen systematisch zu bewerten.

Ein Beispiel dafür sind Lösungen, die digitale Planungswerkzeuge, Nachhaltigkeitsindikatoren sowie Infrastrukturinformationen in bestehende kommunale Systeme integrieren. Dadurch können Städte neue Datenquellen direkt in ihre Planungsprozesse einbinden und Maßnahmen zur Klimaanpassung oder nachhaltigen Stadtentwicklung datenbasiert vergleichen. Die Plattformen sind modular aufgebaut und ermöglichen es, neue Anwendungen oder Datenquellen schrittweise zu integrieren.

Reporting & Digital Twin

Für die transparente Bewertung von Nachhaltigkeitsmaßnahmen entwickelt das Center Lösungen für digitales Monitoring, Reporting und digitale Zwillinge von Infrastrukturen und Gebäuden. Digitale Gebäude-Logbücher und Produktpässe ermöglichen eine strukturierte Dokumentation von Materialeigenschaften, Emissionen und Lebenszyklusdaten.

Diese Informationen werden mit Planungsdaten und Nachhaltigkeitsindikatoren verknüpft und bilden die Grundlage für konsistentes Nachhaltigkeitsreporting sowie für strategische Transformationspfade in Richtung klimaneutraler Städte. Ergänzend dazu ermöglichen digitale Zwillinge die Simulation unterschiedlicher Entwicklungsoptionen, beispielsweise für Energie- oder Infrastrukturmaßnahmen. Städte können dadurch die Auswirkungen geplanter Maßnahmen analysieren und fundierte Entscheidungen für eine langfristig nachhaltige und resiliente Stadtentwicklung treffen.

7 ENABLING DIGITAL TECHNOLOGIES

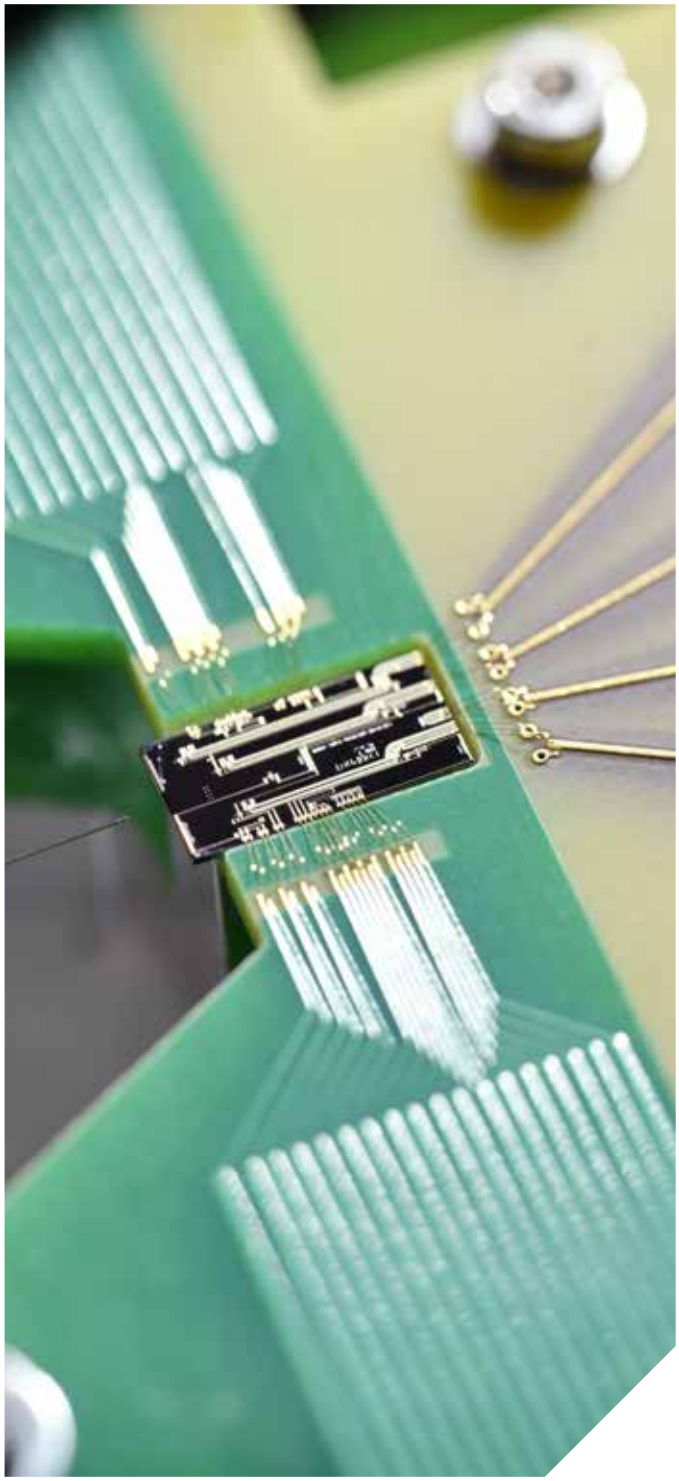
Der Begriff Enabling Digital Technologies umfasst jene strategischen Schlüsseltechnologien, die als technologische Grundlage für künftige sichere, resiliente und souveräne digitale Infrastrukturen dienen. Sie schaffen die Voraussetzungen für Innovation in Industrie, Verwaltung und kritischer Infrastruktur. Gleichzeitig stärken diese Technologien Europas technologische Handlungsfähigkeit sowie digitale Souveränität in gesamtgesellschaftlicher Hinsicht.

Im Fokus stehen dabei drei Kernbereiche. Neue photonische Sensoren ermöglichen hochpräzise Mess- und Detektionssysteme für Anwendungen in Sicherheit, Umweltüberwachung und Industrie. Quantenverschlüsselung sowie Quantenkommunikation: Diese gewährleisten auch im Zeitalter leistungsfähiger Quantencomputer langfristig eine vertrauenswürdige und abhörsichere Informationsübertragung. Modernste Funktechnologien wie 5G und 6G bilden das Rückgrat vernetzter, latenzkritischer und missionsrelevanter Anwendungen. Sie schaffen die infrastrukturelle Basis für datenintensive Echtzeitsysteme. In ihrem Zusammenspiel bilden diese Technologien die Grundlage für robuste, leistungsfähige und zukunftssichere digitale Systeme sowie auch für neue, skalierbare Anwendungen.

Optical Quantum Technologies

Chip-Technologien der nächsten Generation

Traditionelle elektronische Bauelemente stoßen zunehmend an physikalische und technische Grenzen, insbesondere in Bezug auf Geschwindigkeit, Energieeffizienz und Miniaturisierung. Nicht zuletzt durch die steigende Nachfrage nach leistungsfähigeren, energieeffizienten und kompakteren Technologien, wächst somit der Bedarf an innovativen Lösungen wie beispielsweise Photonik-on-the-Chip. Diese Technologie ermöglicht die nächste Generation von Hochleistungsprozessoren und Kommunikationssystemen, die für Anwendungen in Bereichen der Telekommunikation, Sensorik und Quantenkryptographie entscheidend sind. Die Integration von Photonik auf Halbleiterchips – sogenannte Photonic Integrated Circuits (PICs) – bietet eine vielversprechende Lösung, um diese Herausforderungen bei gleichzeitiger Leistungssteigerung zu meistern. Für Österreich ist es als aufstrebender Halbleiterstandort im Rahmen des EU Chips Act entscheidend, in diesen zukunftsweisenden Technologiebereich zu investieren und eine Expertise für den Standort Österreich aufzubauen.



Das AIT Center for Digital Safety & Security treibt mit führender Forschung und innovativen Projekten im internationalen Vergleich die Entwicklung von Photonic Integrated Circuits (PICs) voran. So ist das AIT in prestigeträchtigen Programmen der Photonik-Technologie aktiv und Projektkoordinator des European Innovation Council (EIC) Pathfinder-Projekts QOSiLICIOUS. Darüber hinaus erhielt es den Zuschlag für das „Photonics 4 Quantum" (P4Q) Framework Partnership Agreement im Rahmen des Chips JU Quantum Chip Technology Programs für den Aufbau von Produktionskapazitäten für die Herstellung von photonischen Chips und Komponenten für Anwendungen in der Quantentechnologie. Mit dieser Kompetenz und durch die Etablierung des Chips-Kompetenzzentrums AT-C3 hat sich das AIT auch in der EU Chips Act Initiative positioniert und stellt dieses spezielle Know-how der österreichischen Herstellerindustrie zur Verfügung.

Die Expert:innen des Centers arbeiten derzeit an der Realisierung einer Lichtquelle auf Basis von Silizium. Dieser monolithische Ansatz für quantenoptisch integrierte Schaltungen ist mit den Wafer-Fabriken der Elektronikindustrie zur Gänze kompatibel und erlaubt außerdem die nahtlose Co-Integration von optischen Quantentechnologien in elektronische Prozessoren. Dies stellt künftig eine äußerst kostengünstige Fertigung von chipbasierten, quanten-optischen Systemen in Aussicht, wie sie etwa für die informationstheoretisch sichere Quantenkryptographie benötigt werden. Mit diesen exzellenten Entwicklungen leistet das AIT einen entscheidenden Beitrag zur Stärkung Österreichs als Halbleiterstandort im Rahmen des EU Chips Act.

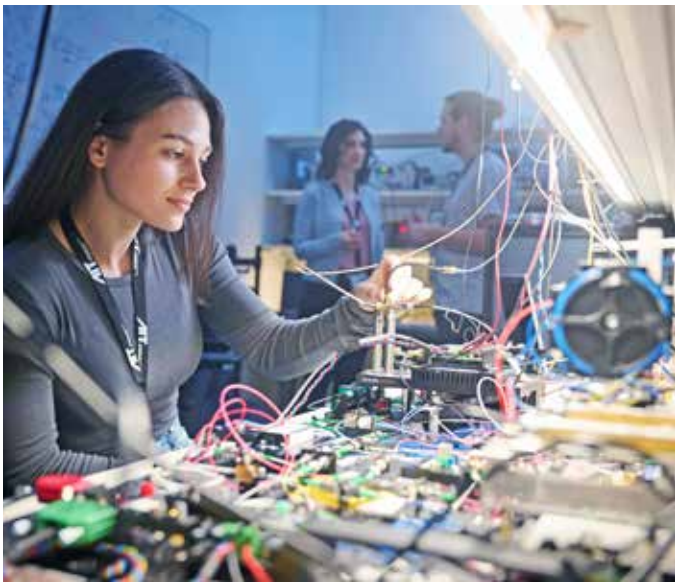
QOSiLICIOUS

AT-C3

Photonik

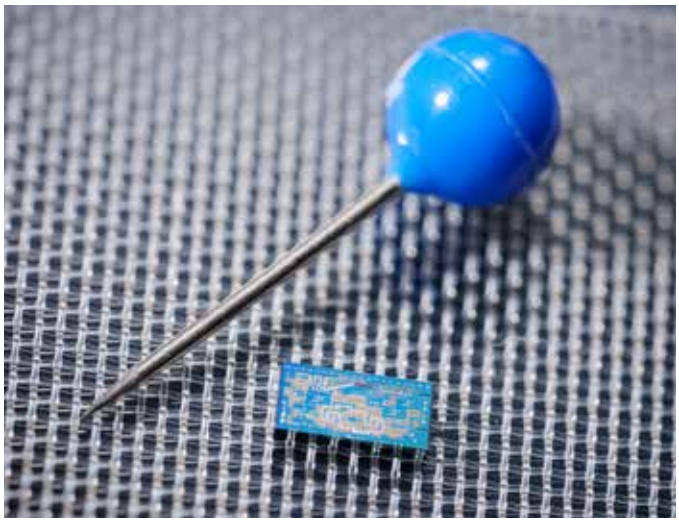
Quantenverschlüsselung

Aufbauend auf der Grundlagenforschung des dafür mit dem Nobelpreis ausgezeichneten Österreichers Anton Zeilinger konnte sich das AIT mit dem Center for Digital Safety & Security im Bereich der Quantentechnologien sehr erfolgreich als essenzieller Know-how-Träger und Technologielieferant für die EU-Technologieumsetzungsstrategie sowie den Aufbau einer europäischen Herstellerindustrie für Quantenverschlüsselung (Quantum Key Distribution – QKD) positionieren. Heute führt das AIT als international führendes Kompetenzzentrum sowohl für terrestrische als auch für satellitenbasierte Quantenkryptographie wesentliche Umsetzungsinitiativen für ein sicheres, vernetztes Europa an, beispielsweise im Rahmen der EU-Programme EuroQCI (Glasfaserinfrastruktur) und IRIS2 (Satelliteninfrastruktur durch die Programme SAGA und EAGLE).



Diese Aktivitäten erfolgen im Rahmen von substanziellen Technologieentwicklungsaufträgen der ESA, von Industrieorganisationen und der Europäischen Kommission für den Aufbau spezieller Test- und Verifikationsfähigkeiten in der EU (Projekt Nostradamus). Dazu gehören die großen Technologie-Pilotvorhaben in allen Mitgliedstaaten wie das Digital Europe Programm (DEP) mit Projekten wie QCI-CAT und PETRUS. Ein weiterer Schwerpunkt liegt auf Projekten für den Aufbau von Technologieanbietern (Zulieferindustrie) im EU-Quantum-Flagship-Programm und im Digital-Europe-Programm, wie beispielsweise eCausis und Quarter. Dazu gehört auch der Aufbau einer Herstellerindustrie in der EU durch EU-Projekte wie Q-Test und Q-Pilot.

Der Aufbau eines quantensicheren Netzwerks in Österreich wurde z. B. bereits mit einem innerstädtischen Rechnernetz zwischen vier Bundesministerien und einer Überlandstrecke von Graz nach Wien erfolgreich demonstriert. Um dabei einem realen Betrieb nahe zu kommen, wurden verschiedenste Anwendungen wie Secret Sharing, Video-Chat und Daten Backups entwickelt. Ihre Sicherung erfolgte mit QKD. Die Expertise des AIT Center for Digital Safety & Security ist auch eine wichtige Grundlage für dedizierte Strategieberatungsaktivitäten im Sinne der EU-Kommission rund um die Entwicklung einer EU-Standardisierungsstrategie sowie einer EU-QKD-Technologiestrategie. Das AIT besitzt in diesem Hochtechnologiebereich ca. 30 Patente.



EuroQCI | IRIS2 | QCI-CAT | PETRUS | Open QKD Technology | Quanten-technologien

Funktechnologien der nächsten Generation

Mit der fortschreitenden Digitalisierung und dem Aufkommen autonomer Systeme steigt der Bedarf an zuverlässigen, sicheren und energieeffizienten drahtlosen Kommunikationslösungen für sicherheitskritische Anwendungen in der Industrie sowie im Straßen-, Schienen- und Luftverkehr. Sicherheitskritische Anwendungen wie autonome Fahrzeuge, Industrie 4.0 oder öffentliche Verkehrssysteme erfordern drahtlose Kommunikationslösungen, die höchste Zuverlässigkeit und Sicherheit gewährleisten. Herkömmliche Funktechnologien stoßen hier an ihre Grenzen, insbesondere wenn es um Latenzzeiten und Ausfallsicherheit geht. Es besteht ein dringender Bedarf an innovativen Technologien, die diese Anforderungen erfüllen und zugleich als Testplattformen für zukünftige Kommunikationsstandards wie 6G dienen.

Das AIT Center for Digital Safety & Security verfügt in Österreich auf dem Gebiet der nächsten Funktechnikgeneration 6G über führende wissenschaftliche und technologische Kompetenzen und ist mit innovativen, zuverlässigen, drahtlosen und energieeffizienten Entwicklungen im Bereich der Kommunikationstechnologien erfolgreich im EU-Industrieökosystem etabliert. Das Center hat weltweit erstmals 6G-Technologiekomponenten mit Software Defined Radio (SDR) Komponenten als Proof of Concept umgesetzt. 6G-Technologiekomponenten sind weitverteilte Antennensysteme, rekonfigurierbare und intelligente Oberflächen und Multiband-Funksysteme. Für diese drei Technologiebereiche wurden Steuer- und Signalverarbeitungsmethoden für integrierte Kommunikation sowie Lokalisierung entwickelt. Als Basistechnologie wurden im Center neuartige Funkkanalmessverfahren und numerische Simulationsmethoden auf der Grundlage geometriebasierter Modelle für 6G-Systeme erforscht. Gleichzeitig wurden Testmethoden für Funksysteme etabliert, die auf maschinellem Lernen basieren. Weiters leitet das AIT durch das Center die internationale Standardisierungsaktivität im Rahmen von IEEE P1944 für geometriebasierte Funkkanalmodelle, die ein zentraler Bestandteil der Forschungs- und Testmethoden für 6G-Kommunikations- und Lokalisierungssysteme sind.

Wichtige Anwendungsfälle sind der autonome Zugverkehr, autonome Güterwaggons, der sicherere Betrieb von autonomen Fluggeräten (UAV), eine verbesserte Verkehrssicherheit durch Sensordatenaustausch zwischen den Straßenfahrzeugen u. v. m. Weiters werden Funksysteme in Zukunft neben der Datenkommunikation auch Lokalisierungsfähigkeiten anbieten. Vor diesem Hintergrund konnte das AIT erfolgreich F&E-Kooperationen mit der österreichischen und EU-Leitindustrie etablieren – etwa mit Siemens, den ÖBB, AVL und Ericsson sowie Thales. Darüber hinaus besitzt das AIT in diesem Hochtechnologiebereich bedeutende Patente.

Drahtlose Kommunikation

8 INITIATIVEN UND PLATTFORMEN

Vertrauenswürdige Digitalisierung, digitale Souveränität und gesellschaftliche Resilienz entstehen nicht isoliert, sondern durch starke Netzwerke, gemeinsame Plattformen und internationale Zusammenarbeit. Technologische Innovation muss dabei mit regulatorischen Anforderungen, gesellschaftlicher Verantwortung und praktischer Umsetzbarkeit verbunden werden. Strategische Initiativen und Kooperationsplattformen spielen daher eine zentrale Rolle, um Akteure aus Forschung, Industrie, öffentlicher Verwaltung und internationaler Politik zusammenzuführen und Wissen und Kompetenzen auszutauschen.

Mit Initiativen wie dem Gaia-X Hub Austria, dem International Digital Security Forum (IDSF) und der PeaceTech Alliance werden konkrete Räume für Austausch, Community-Building und die Entwicklung vertrauenswürdiger digitaler Ökosysteme geschaffen. Sie leisten einen aktiven Beitrag dazu, europäische Werte, technologische Innovation und internationale Kooperation im digitalen Raum nachhaltig zu stärken und in die praktische Umsetzung zu überführen.

Gaia-X Hub Austria

Daten sind zu einer strategischen Ressource für Wirtschaft, Verwaltung und Gesellschaft geworden. Gleichzeitig wächst das Bewusstsein, dass ihre Nutzung klare Regeln, Vertrauen und technologische Souveränität erfordert. Denn Organisationen stehen zunehmend vor der Aufgabe, Daten über Unternehmens-, Sektor- und Ländergrenzen hinweg zu teilen, ohne dabei die Kontrolle, Compliance und ebenso die Wettbewerbsfähigkeit zu verlieren. Zudem stellen Vertrauen, klare Rollen sowie die technische Durchsetzbarkeit gerade in kritischen Bereichen wie Energie, Industrie, Sicherheit oder öffentlicher Verwaltung keine theoretischen Anforderungen, sondern operative Notwendigkeiten dar. Datenräume müssen daher nicht nur konzeptionell überzeugen, sondern im realen Betrieb skalieren, regulatorische Anforderungen erfüllen und einen messbaren Mehrwert liefern.

Der Gaia-X Hub Austria nimmt hier eine Schlüsselrolle als zentraler Wegbereiter für vertrauenswürdige, interoperable Datenräume ein, wodurch europäische Werte wie Transparenz, Sicherheit und Selbstbestimmung praktisch umsetzbar werden. Zur Unterstützung der Datensouveränitätsziele in der EU und zur Förderung der Entwicklung eines neuen, datengetriebenen Ökosystems hat das AIT mit dem Center for Digital Safety & Security im gemeinsamen Auftrag des Bundesministeriums für Innovation, Mobilität und Infrastruktur (BMIMI) sowie des Staatssekretariats für Digitalisierung im Bundeskanzleramt (BKA) erfolgreich und maßgeblich den Gaia-X Hub Austria etabliert. Er dient der Beschleunigung europäischer Datenökosysteme für ökonomische, ökologische und gesellschaftliche Wertschöpfung und hat sich somit als Brückenbauer zwischen dem europäischen Rahmenwerk und nationaler Umsetzung bewährt. Durch gezielte Vernetzung von Wirtschaft, Forschung, Verwaltung und Politik unterstützt der Hub die konkrete Anwendung von Gaia-X-Prinzipien in realen Projekten.

Darüber hinaus hat sich das AIT Center auch in der EU Gaia-X Initiative als Board-Mitglied steuernd etabliert. Initiativen wie EDDIE (Energiedatenraum), PASSAT (Digital Product Passport) und UNDERPIN (Manufacturing) zeigen anschaulich, dass Datenräume in Österreich nicht mehr Pilotversuche sind, sondern einen praktischen Mehrwert in unterschiedlichen Sektoren liefern können. Als weiterer Meilenstein ist der DPP-Demonstrator aus dem Projekt BatWoMan zu nennen, der als Blaupause für die Umsetzung eines Batteriepasses dient. Der Demonstrator zeigt konkret, wie normative Anforderungen aus aktuellen und zukünftigen EU-Regularien, insbesondere im Kontext des Digital Product Passport, technisch umgesetzt und in bestehende Wertschöpfungsketten integriert werden können.

Auch im Sicherheitsbereich unterstreichen KIRAS-Projekte wie ASOC und DAGMAR, dass souveräne Datenräume ein zentrales Element zur Bewältigung hybrider Bedrohungen und zum Schutz kritischer Infrastrukturen darstellen. Im Kontext der PeaceTech Alliance, gemeinsam mit dem Austrian Center for Peace (ACP) und weiteren Partnern, wird darüber hinaus sichtbar, wie Datenräume Vertrauen, Kooperation und Resilienz auch in internationalen sowie sicherheitspolitisch sensiblen Umfeldern unterstützen können.

Der Hub positioniert sich damit nicht nur als Koordinationsstelle, sondern als aktiver Beschleuniger für die Umsetzung digitaler Souveränität in Österreich, mit klarer Orientierung an realen Anwendungsfällen und regulatorischer Umsetzbarkeit.

Mit der Gaia-X Academy stellt der Hub darüber hinaus ein frei zugängliches, online-basiertes Schulungsprogramm zur Verfügung, das Unternehmen, Organisationen und Einzelpersonen praxisnah an die Konzepte, Technologien und Governance-Modelle von Datenräumen heranführt. Damit wird gezielt Know-how aufgebaut, um den Einstieg in Gaia-X-konforme Datenökosysteme zu erleichtern und die Breitenwirkung zu erhöhen. Diese Entwicklungen unterstreichen den Anspruch des Gaia-X Hub Austria, nicht nur eine strategische Orientierung zu geben, sondern Unternehmen ganz konkret bei der Umsetzung regulatorischer Vorgaben und beim Aufbau zukunftsfähiger, souveräner Datenräume zu unterstützen.

gaia-x Hub Austria

EDDIE

PASSAT

UNDERPIN

BatWoMan

ASOC

DAGMAR

Gaia-X Academy

Gaia-X Hub AT

International Digital Security Forum (IDSF)

Sicherheit ist eine zentrale Voraussetzung für den Einsatz digitaler Technologien. Neue Entwicklungen wie Künstliche Intelligenz (KI), das Internet der Dinge (IoT), biometrische Verfahren für das digitale Identitätsmanagement, cloudbasierte Dienste und globale Netzwerke eröffnen innovative Anwendungsmöglichkeiten, entfalten jedoch zugleich disruptive Wirkungen auf bestehende Systeme, Märkte und gesellschaftliche Strukturen. Insbesondere die Cybersicherheit stellt dabei hohe Anforderungen an Systementwickler, Serviceanbieter und Nutzer:innen.

Mit der zunehmenden Demokratisierung digitaler Technologien entstehen neue Bedrohungsszenarien, deren Reichweite und Skalierbarkeit klassische Schutzmechanismen auf organisatorischer wie staatlicher Ebene zunehmend an ihre Grenzen bringen. Das sich wandelnde Bedrohungsumfeld erfordert daher ein neues Verständnis kritischer Infrastrukturen sowie innovative Ansätze zur Stärkung ihrer Resilienz. Zugleich gewinnen internationale Koordination, vertrauensbildende Maßnahmen und ein strukturierter Informationsaustausch an Bedeutung, um auf globale Risiken angemessen reagieren zu können. All dies muss jedoch im Einklang mit universellen Menschenrechten erfolgen, die in erster Linie sowohl die Wahrung der Meinungsfreiheit als auch das Recht auf Privatsphäre garantieren.

Vor diesem Hintergrund wurde im Jahr 2020 mit dem International Digital Security Forum (IDSF) ein neues Format für internationalen Austausch und Community Building initiiert, das im Juni 2025 bereits in seiner 4. Ausgabe in Wien organisiert wurde. Das IDSF wird vom AIT Austrian Institute of Technology mit Unterstützung des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA) sowie weiterer zentraler österreichischer Bundesministerien organisiert. Die Durchführung erfolgt in enger Zusammenarbeit mit der ARGE Sicherheit und Wirtschaft der Wirtschaftskammer Österreich, dem Kompetenzzentrum Sicheres Österreich (KSÖ) und der Agency for Economic Cooperation and Development (AED) in Kooperation mit internationalen Partnerorganisationen.

INTERNATIONAL
DIGITAL
SECURITY
FORUM
VIENNA

Das IDSF basiert auf drei zentralen Säulen: Erstens widmet es sich den sicherheits- und gesellschaftspolitischen Herausforderungen, die aus dem Einsatz neuer digitaler Technologien entstehen. Zweitens bringt es gezielt alle relevanten Akteure der digitalen Sicherheitslandschaft zusammen, beginnend von staatlichen Entscheidungsträger:innen auf nationaler, europäischer und internationaler Ebene, die aus den Bereichen Industrie, Forschung, Wissenschaft und Medien sowie aus der Zivilgesellschaft kommen. Drittens setzt das Forum auf innovative Formate und Werkzeuge für Wissensaustausch, Diskussion und Bewusstseinsbildung, die Präsenzformate mit digitalen Präsentationsmöglichkeiten verbinden.

Diese drei Säulen bilden die Grundlage für den Anspruch, das IDSF als international einzigartigen Dialograum zu etablieren. Über die einzelne Veranstaltung hinaus trägt das Forum zum Aufbau einer weithin anerkannten Plattform für internationale Diskussion und Zusammenarbeit bei. Ziel ist es, gemeinsame Rahmenbedingungen, Regeln und ein gemeinsames Verständnis zu fördern, damit digitale Technologien langfristig dem Menschen und der Gesellschaft dienen.

Wien als Veranstaltungsort unterstreicht diesen Anspruch. Die internationale Rolle Österreichs und seine Tradition als neutraler Vermittler schaffen ideale Voraussetzungen für eine offene, grenzüberschreitende und vertrauensvolle Diskussion im globalen Kontext digitaler Sicherheit.

IDSF.IO

PeaceTech Alliance

Die PeaceTech Alliance ist eine internationale, gemeinnützige Plattform, die sich dem verantwortungsvollen Einsatz digitaler Technologien für Friedensförderung, Konfliktprävention und gesellschaftliche Resilienz widmet. Sie geht von der Überzeugung aus, dass Technologie ein erhebliches Potenzial zur Unterstützung von Friedensprozessen besitzt, beispielsweise durch bessere Informationsgrundlagen, den Einsatz Künstlicher Intelligenz (KI), neue Formen der Zusammenarbeit oder den Kapazitätsaufbau lokaler Akteure. Gleichzeitig macht sie deutlich, dass diese Potenziale nur dann wirksam werden, wenn technologische Innovationen zugänglich sind und kontextsensibel sowie wertebasiert gestaltet werden.

Die PeaceTech Alliance wurde 2025 vom AIT gemeinsam mit dem Gaia-X Hub Austria im Rahmen des 4. International Digital Security Forum (IDSF) in Wien ins Leben gerufen. Sie baut auf einem starken interdisziplinären Partnernetzwerk auf, das Österreichs besondere Rolle an der Schnittstelle von Friedensförderung, Diplomatie, Wissenschaft und Technologie widerspiegelt. Zu den initialen Partnern zählen unter anderem das Austrian Center for Peace, das International Institute for Peace, die Open Knowledge Foundation, die Diplomatische Akademie Wien sowie akademische Einrichtungen wie die Universität Innsbruck, die Karl-Franzens-Universität Graz und die Donau-Universität Krems. Internationale Perspektiven werden unter anderem durch die Open Knowledge Foundation eingebracht.

Im Zentrum der Aktivitäten stehen Austausch, Kompetenzen und Zusammenarbeit. Die PeaceTech Alliance bietet Veranstaltungen, Workshops und Trainingsformate sowie praxisnahe Inhalte über Blogs, Podcasts und Toolkits, die technologische Ansätze verständlich aufbereiten und konkrete Anwendungsbeispiele sichtbar machen. Ergänzend werden digitale Projekte und offene Werkzeuge entwickelt, die Friedensakteur:innen dabei unterstützen, ihre Arbeit sicherer, wirkungsvoller und nachhaltiger zu gestalten. Ein besonderer Schwerpunkt liegt auf der Einbindung der Zivilgesellschaft als Mitgestalterin technologischer Lösungen und nicht nur in ihrer Rolle als deren Anwenderin.

Ein weiterer Kernbereich der Initiative ist der Aufbau föderierter, vertrauenswürdiger Datenräume für friedens- und sicherheitsrelevante Anwendungsfälle. Aufbauend auf den Prinzipien von Gaia-X verfolgt die PeaceTech Alliance das Ziel, souveränen Datenaustausch zu ermöglichen sowie eine Zusammenarbeit zu fördern, ohne dabei die Kontrolle, die Verantwortung sowie den Datenschutz zu gefährden. Solche Strukturen schaffen die Grundlage für Vertrauen zwischen staatlichen, zivilgesellschaftlichen und internationalen Akteuren in einer zunehmend datengetriebenen Welt.

Verankert im österreichischen Selbstverständnis von Neutralität und Dialog und getragen von einem wachsenden Netzwerk aus nationalen und internationalen Partnern positioniert sich die PeaceTech Alliance als offener Kooperationsraum für verantwortungsvolle digitale Innovation. Sie leistet damit einen Beitrag zur Weiterentwicklung eines humanen, inklusiven und zukunftsorientierten Verständnisses von Technologie mit dem klaren Anspruch, digitale Werkzeuge konsequent in den Dienst von Frieden, Vertrauen und gesellschaftlicher Stabilität zu stellen.

PeaceTech
Alliance

9 INTERNATIONALES NETZWERK

Digitale Souveränität, technologische Resilienz und globale Wettbewerbsfähigkeit erfordern heute starke internationale Partnerschaften und vernetzte Innovationsökosysteme. Eine zentrale Grundlage, um neue Technologien vertrauenswürdig, interoperabel und skalierbar zur Anwendung zu bringen, ist die enge Zusammenarbeit mit europäischen Institutionen, internationalen Organisationen, Industriepartnern sowie nationalen Behörden.

Durch die aktive Mitgestaltung internationaler Forschungs-, Industrie- und Standardisierungsinitiativen sowie die Zusammenarbeit mit führenden Technologie- und Sicherheitsorganisationen ist das AIT Austrian Institute of Technology mit dem Center for Digital Safety & Security international stark verankert. Über dieses Netzwerk kann österreichische Technologiekompetenz in strategischen Zukunftsfeldern wie Cybersicherheit, Quantentechnologien, Datenräume, Künstliche Intelligenz und digitale Sicherheit nachhaltig auf nationaler und europäischer Ebene positioniert werden.

Internationales Netzwerk

Generell besitzt das AIT Center for Digital Safety & Security in nationalen und internationalen Innovationsprogrammen wie KIRAS und Horizon Europe eine anerkannte Position und ist gestaltender Teil von Industrie- und Forschungsinitiativen wie beispielsweise Quantum Communication Infrastructure Europe (QCI), European Cyber Security Organisation (ECSO), Public Safety Communication Europe (PSCE), Electronic & Software Based Systems (ESBS) oder Task Force der europäischen Forschungsorganisationen im Sicherheitskontext (EARTO/EUROTECH). Dazu kooperiert das Center mit internationalen Organisationen wie der Internationalen Atomenergiebehörde (IAEA), der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), dem United Nations Office on Drugs and Crime (UNODC), dem United Nations Office of Counter-Terrorism (UNOCT) sowie dem Vienna Center for Disarmamanet and Non-Proliferation (VCDNP). Auf nationaler Ebene sind das Bundesministerium für Inneres (BMI) sowie das Bundesministerium für Landesverteidigung (BMLV) wichtige Partner. Damit wurde eine wesentliche Grundlage geschaffen, um technologische Innovationen aus Österreich sowie die dazugehörigen Kompetenzen international zu verankern, wie im folgenden Überblick zusammengefasst wird.

Das AIT Austrian Institute of Technology ist mit dem Center for Digital Safety & Security einer der Schlüsselakteure in der europäischen EuroQCI sowie IRIS2-Community und wird seitens der Europäischen Kommission (EC) auch als wichtiger Stakeholder für die Umsetzung der Ziele der EC im Bereich der Quantenkommunikation gesehen. Das zeigt sich durch eine breite Verankerung in allen Bereichen der EU-Programme, durch die Industriekooperationen mit der EU-Leitindustrie wie z. B. Deutsche Telekom, Thales und Airbus sowie auch durch die explizite Einbindung als Strategieberater für die EC. Weiters konnte sich das Center in diesem Bereich erfolgreich in der EU-Weltraum-/Satellitenindustrie als Technologielieferant für die ESA und für EU-Leitindustriepartner wie z. B. Deutsche Telekom (D), Thales (F), OHB (D), SES (Lux) und Thales Alenia-Space (I) etablieren.

Diese starke Kompetenz im Bereich der Quantentechnologien, verbunden mit den Kompetenzen in Photonik-Technologien, der 6G-Funktechnik sowie einer sicheren Embedded Systementwicklung und Cyber Security bildet auch die Grundlage für die Positionierung des AIT in der österreichischen Electronic & Software Based Systems (ESBS)-Community. Gemeinsam mit Halbleiterschlüsselindustrien wie Infineon, AMS/Osram, AT&S und AVL fördert das AIT so den High-Tech-Standort Österreich.

Für die Umsetzung der Datensouveränitätsziele der EU hat sich das AIT mit dem Center for Digital Safety & Security erfolgreich im EU-Netzwerk für den Aufbau föderierter Datensysteme etabliert. Österreich ist durch die Aktivitäten des Centers anerkannter Stakeholder im Netz der internationalen Gaia-X Hubs und hat sich auch als wichtiger nationaler Leitakteur für die Datenplattform-Szene in Österreich positioniert. Diese Entwicklung wird durch eine erfolgreiche Kooperation mit dem Bundesministerium für Innovation, Mobilität und Infrastruktur (BMIMI) sowie dem Staatssekretariat für Digitalisierung belegt. Weiters ist die österreichische Forschungseinrichtung auch im Board der EU-Gaia-X-Initiative vertreten.

Zur Unterstützung der digitalen Transformation, vor allem in Bezug auf die Themen Cyber-Security, Künstliche Intelligenz und Sensorsysteme (IoT), kooperiert das AIT mit der nationalen Industrie und bekleidet in den maßgeblichen Netzwerk-Communities der Plattform Industrie 4.0 Austria aktive Funktionen.

Im Bereich Cyber Security hat das AIT eine erfolgreiche Positionierung im Netzwerk der internationalen Organisationen für Sicherheit etabliert. Das AIT und damit Österreich ist derzeit das einzige „Collaborating Centre" der IAEA für IT-Sicherheit. Das AIT Center führt darüber hinaus gemeinsam mit dem World Institute for Nuclear Security (WINS) und dem United Nations Office for Counter Terrorism (UNOCT) laufend internationale Trainings durch. Darauf aufbauend präsentiert sich das AIT auch als wichtiger Netzwerkpartner für das österreichische Außenministerium (BMEIA). Auf nationaler Ebene profilierte sich das AIT mit dem Center for Digital Safety & Security als anerkannter Experte für Cyber Security. Das manifestiert sich durch die aktive Einbindung in die wichtigen nationalen Netzwerkorganisationen wie dem Kompetenzzentrum Sicheres Österreich (KSÖ), der Cyber-Security-Plattform (CSP) des Bundeskanzleramts, der Digital City Vienna, dem Vienna Cybersecurity and Privacy Research Cluster (ViSP) und schließlich durch die Etablierung als Umsetzungspartner der laufenden nationalen Cyber-Security-Planspiele des Bundesministeriums für Inneres (BMI) mit dem nationalen Netzwerk der Betreiber kritischer Infrastrukturen.

Digital Factory Vorarlberg – Ein Wissenszentrum für Digitalisierung

Ein interdisziplinäres Projektteam bestehend aus FH Vorarlberg und dem AIT Center for Digital Safety & Security gründete unter Koordination der Wirtschafts-Standort Vorarlberg GmbH (WISTO) mit der Digital Factory Vorarlberg ein spezielles Forschungszentrum für den Standort Vorarlberg. Die Verknüpfung der regionalen Hochschule mit den Kompetenzen des größten außeruniversitären Forschungszentrums Österreichs eröffnet den Zugang zu internationalen Forschungsnetzwerken, schafft überbetriebliche Forschungskapazität und -kompetenz und macht diese für Vorarlberger Unternehmen zugänglich.

EuroQCI | ECSO | PSCE | ESBS-Austria | Industrie 4.0 Österreich | EARTO | Gaia-X | Digital Factory Vorarlberg

10 AUSGEWÄHLTE FORSCHUNGS-INFRASTRUKTUREN

Das Center verfügt über eine starke Ausrichtung auf softwarebasierte Entwicklungs- und Forschungstätigkeiten. Für drei ausgewählte Hochtechnologiebereiche wurden gezielt spezialisierte Forschungsinfrastrukturen aufgebaut, die als Grundlage für international konkurrenzfähige Spitzenforschung dienen und zugleich eine hohe Zahl an Kooperationen mit Wissenschafts- und Industriepartnern ermöglichen.

OQC Lab

Photonics & Quantum Communication Laboratory

Das Photonics & Quantum Communication Laboratory adressiert Technologien, die auf der Nutzung von Licht basieren. Die Aktivitäten der Forschungsgruppen in diesem Bereich reichen von photonisch integrierten Schaltungen auf Chipebene über die Systemintegration von optischen und elektronischen Komponenten bis hin zur Demonstration neuer Anwendungen in der Telekommunikation, Quantenoptik und Sensorik.

Das Forschungslabor verfügt über eine Probestation zur Ansteuerung und Vermessung photonischer Chips, eine breite Palette von Instrumenten zur optischen und hochfrequenten Signalerzeugung und -analyse von Nanometern bis Terahertz sowie über supraleitende Nano-Wire Detektoren zur Messung von Einzelphotonen.

Durch die aufgebaute Laborinfrastruktur im Center for Digital Safety & Security ist das AIT in der Lage, nach dem Design von Komponenten und Systemen der Quantenkommunikation diese zu vermessen, aber auch das Labor in Europa als Testlaboratorium zur Verfügung zu stellen. Bei den quantenoptischen Komponenten und Systemen handelt es sich um unterschiedliche Arten von QKD-Implementierungen, wie beispielsweise Transmitter und Receiver für CV-, DV-, verschränkungsbasierte, und Measurement-Device-Independent-QKD-Systeme – „on the chip“ oder als optische Systeme, weiters um Quantenzufallszahlengeneratoren, neuromorphe optische Chips und ähnliche Subsysteme.

Radio Frequency Laboratory

Sichere und gesicherte elektronische Kommunikationsverbindungen sind eine zentrale Voraussetzung für eine moderne Gesellschaft. Die Forschungsgruppe Wireless Communication and Sensing arbeitet an neuen Methoden zur Ausnutzung der physikalischen Eigenschaften drahtloser Kommunikationsmedien, um Sicherheit und Schutz zu gewährleisten und die Position von Objekten zu bestimmen.

Im Bereich der drahtlosen Kommunikation werden neuartige Kommunikations- und Lokalisierungsmethoden für 5G-/6G-Systeme entwickelt, die ultrazuverlässige und latenzarme Kommunikationsverbindungen mit einer genauen Positionsbestimmung ermöglichen. Sie sorgen z. B. dafür, dass in Produktionsumgebungen Kabel durch ein drahtloses System ersetzt werden oder autonome Fahrzeuge und Züge zuverlässig fahren können.

Diese Laborinfrastruktur ermöglicht die Bearbeitung eines weiten Bereichs an Forschungs- und Anwendungsfragen für Kommunikations- und Lokalisierungssysteme. So können beispielsweise Funkkanal-Emulationen für „Hardware in the Loop“-Tests angeboten werden. Auch Funksysteme im Bereich der Millimeterwelle, die mittels neuartiger rekonfigurierbarer und intelligenter Oberflächen Positionen von Objekten in Innenräumen auf den Zentimeter genau bestimmen können, gehören dazu.

RF Lab

AIT Cyber Range – Test & Training Center

Aufbauend auf der Technologie- und Forschungskompetenz des AIT und dessen Auftrag, die österreichische Gesellschaft, kritische Infrastrukturanbieter und Unternehmen zu unterstützen, werden regelmäßig Cyber Security Trainings und Übungen durchgeführt. Dafür wurde eine einzigartige digitale und hybride Simulationsplattform, die AIT Cyber Range entwickelt. Seit 2017 werden in Kooperation mit dem Kompetenzzentrum Sicheres Österreich (KSÖ) nationale Planspiele mit der öffentlichen Hand sowie Stakeholdern aus Wirtschaft und Industrie durchgeführt. Die AIT Cyber Range entwickelte sich seither mit ihrem Team zu einer Einrichtung von Weltrang. Entsprechend dieser Entwicklung fungiert das AIT gegenwärtig als das das weltweit einzige IAEA „Collaboration Centre" zum Thema Cyber Security für die nukleare Sicherheit und unterstützt hier durch das Center globale Trainingsaktivitäten.

Diese Ausbildungs- und Trainingsinfrastruktur stellt eine komplementäre Ergänzung der Forschungsaktivitäten dar, die es ermöglicht, gemeinsam mit Infrastrukturbetreibern, Herstellern und Sicherheitsbeauftragten neue Verteidigungstechnologien sowie Bedrohungsszenarien zu evaluieren und darauf aufbauend konkrete praktische Fähigkeiten aufzubauen.

AIT Cyber Range

11 ZERTIFIZIERUNGEN

Um Forschung und Entwicklung entsprechend den steigenden Sicherheitsanforderungen von Behörden und Kunden aus der Industrie im Bereich der Digitalisierung unter höchsten Anforderungen an die Informationssicherheit durchführen zu können, hat das AIT Center spezielle Prozesse und Kompetenzen etabliert sowie eine entsprechende Sicherheitsinfrastruktur aufgebaut. Dadurch ist es befähigt, an klassifizierten Projekten auf dem Sicherheitsniveau „EU-Restricted“ zu arbeiten. In diesem Zusammenhang hat das AIT auch die erforderliche Zertifizierung durch die österreichischen Behörden erlangt.

Dank der umfassenden Expertise im Umgang mit klassifizierten Informationen, der behördlichen Zertifizierung durch das Bundesministerium für Landesverteidigung (BMLV) sowie den damit verbundenen besonderen Sicherheitsmaßnahmen in der Organisation, zu denen auch Sicherheitsüberprüfungen der Mitarbeiter:innen gehören, ist das AIT Center for Digital Safety & Security in der Lage, vertrauliche und sicherheitsrelevante Forschungsprojekte rechtskonform und mit höchster Integrität umzusetzen. Diese Voraussetzungen bilden eine zentrale Grundlage für die enge Zusammenarbeit mit nationalen und internationalen Behörden sowie mit Industriepartnern, die höchste Anforderungen an den Schutz sensibler Daten und Informationen stellen.

Bundesministerium Innovation, Mobilität und Infrastruktur

Bundesministerium Finanzen

KIRAS Sicherheitsforschung

FORTE arma et scientia ex officio

K-PASS

FFG Forschung wirkt.

Funded by the European Union

Bundeskanzleramt

Bundesministerium Inneres

Bundesministerium Landesverteidigung

Durch die enge Zusammenarbeit mit öffentlichen Behörden und österreichischen Unternehmen konnte das AIT Center for Digital Safety & Security besondere Kompetenzen, Fähigkeiten und neue technologische Lösungen in mehreren Bereichen entwickeln. Dabei bilden die nationalen Sicherheitsforschungsprogramme KIRAS, KPASS (für Cybersicherheit) und FORTE eine wichtige Grundlage, um international führende Initiativen zu starten.

Die in dieser Publikation dargestellten Aktivitäten und Entwicklungen wurden zudem durch starke strategische Partnerschaften sowie weitere nationale und internationale Förderprogramme maßgeblich mitgestaltet.

Unser besonderer Dank gilt den Fördergeber:innen sowie den zahlreichen Partner:innen aus Wirtschaft, Industrie, Wissenschaft und Öffentlicher Hand, die durch ihr Engagement und ihre langfristige Unterstützung einen wesentlichen Beitrag zur Weiterentwicklung vertrauenswürdiger digitaler Sicherheitslösungen und zur Stärkung digitaler Souveränität in Österreich und Europa leisten.

IMPRESSUM

Herausgeber, Medieninhaber
AIT Austrian Institute of Technology GmbH
Giefinggasse 4, A-1210 Wien
Marketing & Communications
Center for Digital Safety & Security
news.dss@ait.ac.at I www.ait.ac.at/dss

Bildmaterial
AIT Austrian Institute of Technology GmbH
Getty Images

Erscheinungsort
Wien, Juni 2026

Für den Inhalt verantwortlich:

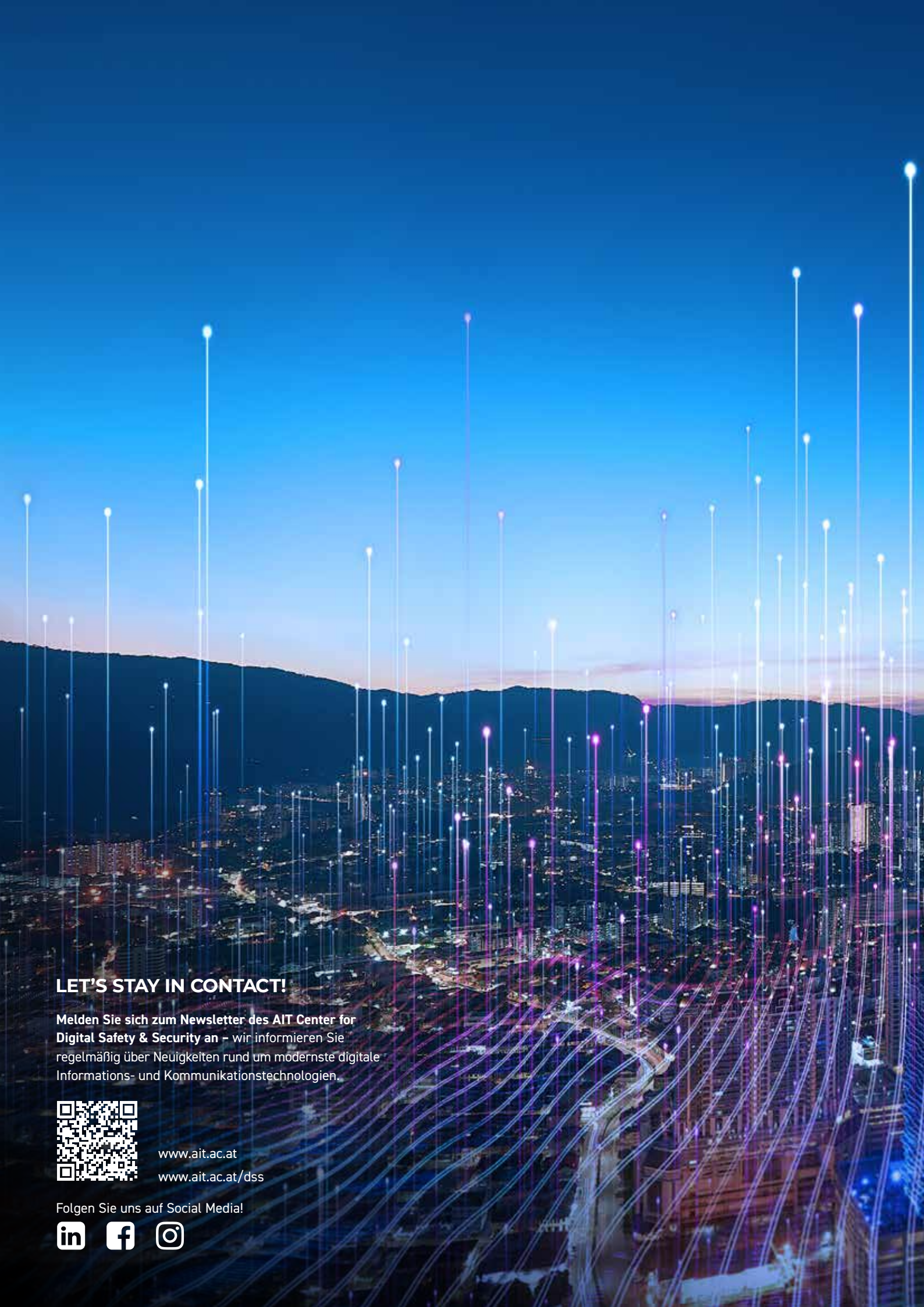
Redaktionsteam
Helmut Leopold
Michael W. Mürling
Mario Drobics
Ross King
Martin Stierle
Hannes Hübel

Design, Gestaltung und Satz
Cayenne Marketingagentur GmbH

produziert nach den Richtlinien des Österreichischen Umweltzeichens, Gradwohl Printproduktionen Ges.m.b.H., UW 1506

WE TURN RESEARCH INTO INNOVATION
BY BRIDGING SCIENCE AND THE ECONOMY
TO SHAPE TOMORROW'S WORLD.

www.ait.ac.at



LET'S STAY IN CONTACT!

Melden Sie sich zum Newsletter des AIT Center for Digital Safety & Security an – wir informieren Sie regelmäßig über Neuigkeiten rund um modernste digitale Informations- und Kommunikationstechnologien.

www.ait.ac.at
www.ait.ac.at/dss

Folgen Sie uns auf Social Media!