

RESPONSIBLE DIGITALIZATION FOR DIGITAL SOVEREIGNTY

Strengthening Resilient Societies and Global Competitiveness
through Trusted Technologies “Made in Austria”

Center for Digital Safety & Security
AIT Austrian Institute of Technology
English Edition

WE MAKE INNOVATION
A DRIVING FORCE
IN EUROPE.



www.ait.ac.at

PREFACE

Digital sovereignty as a new necessity for global competitiveness and a democratic society.



European system manufacturers, network operators and service providers have until now placed the focus of their digitalisation strategies primarily on cost reduction and efficiency gains. Outsourcing and the transfer of competence have been the key mechanisms for the further development of enterprises and public institutions. However, this development has led to fundamental dependencies on continuously and cheaply available digital supply chain products and providers.

Consequently, the economy now faces the new challenge of managing more complex and fragile supply ecosystems in order to remain internationally competitive. Digital sovereignty – i.e. the ability to act autonomously – has become a new prerequisite for a functioning global economy, yet it also determines the sovereign freedom of action of entire countries. The latter forms the basis for democratic, peaceful social structures. Furthermore, we need clear and stable data sovereignty to address the growing importance and dominance of data collections. A lack of data sovereignty (digital autonomy) jeopardises personal integrity, undermines democratic structures and prevents the emergence of new data-driven business models.

Today, only a handful of companies store and process the majority of global information collections at a digital level – the data representing the raw material for digital business models and AI training. These global infrastructures, which have a monopolistic character, restrict the participation of many actors in an open global ecosystem and hinder competition. Even more seriously, this process increasingly restricts our ability to use and process our own data in a self-determined manner.

In the public sector in particular, digital sovereignty requires the responsible development of digital solutions that reconcile technological capabilities with legal, ethical and societal requirements. Digital systems must be designed not only to be efficient, but also to be trustworthy, transparent and secure. Only if data protection, transparency, resilience and fundamental democratic values are integrated from the outset can digitalisation realise its full potential and strengthen the trust of citizens, the business sector and institutions alike.

This entails a particular responsibility, especially for government and public sector applications: digital systems must not be designed solely with efficiency in mind, but they must systematically take into account strategic resilience, legal compliance, ethical standards and societal impacts. Only in this way can sustainable infrastructures be created that guarantee security, safeguard democratic principles and ensure the state's long-term capacity to act.

Innovation arises from the necessary interaction among technology manufacturers, providers, industry, research and the authorities. It is only through this close cooperation that sustainable and scalable solutions become possible which are not only effective at a national level but can also hold their own on the global stage. Digital sovereignty therefore requires a strong innovation ecosystem that combines the highest possible technological quality with strategic cooperation.

Consequently, we urgently need the expertise to assess and sustainably safeguard the trustworthiness and integrity of technical systems. This is not about protectionism or developing everything in-house, but about securing a fundamental freedom of action that, in an emergency or for strategic reasons, allows us to fall back on alternatives in line with the central function of free market economies.

The European Commission is responding to this dynamic with specific EU innovation and research programmes aimed at strengthening digital sovereignty, with a view to establishing strategic technologies and capabilities such as AI, cyber security, quantum technologies and microchips within the EU in a globally competitive manner. In addition, the EU is pursuing a new data strategy and, through the Data Act, Data Governance Act and the AI Act, is establishing clear, legally binding rules for transparency, sovereign data processing and fair data trading.

A strong, self-reliant economy and the effective implementation of the European Commission's innovation programmes depend on robust research and technology organisations. These organisations must act as a neutral innovation infrastructure for industry, the

public sector, and academia. They must also ensure the competitive application of key European technologies.

Furthermore, there is a growing momentum to deploy collaboratively created, publicly funded or industrially developed open-source technologies more widely in businesses and public administration. The Gaia-X open-source and standardisation initiative, driven primarily by EU industry, is laying the groundwork for establishing new data markets (data spaces) in a global context, based on distributed data storage and enabling secure and trustworthy data exchange.

By confidently embracing these new approaches and making our IT systems more resilient through European innovation, we will safeguard our autonomous freedom of action and sustainably strengthen both our economy and our society. This will enable global economic relations to be conducted on an equal footing.

Helmut Leopold

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

INTRODUCTION

With more than 1,600 employees, the AIT Austrian Institute of Technology is Austria's largest research and technology organisation and focuses on the two interlinked research priorities of "sustainable and resilient infrastructures", particularly in the areas of energy, transport and health, and the "digital transformation of industry and society". In doing so, AIT is working closely together with universities, industry and public institutions. Through research and technological developments at AIT, fundamental innovations are realised for the next generation of infrastructure technologies in the fields of Energy, Transport Technologies, Health & Bioresources, Digital Safety & Security, Vision, Automation & Control, and Technology Experience. These scientific research areas are complemented by expertise in the field of Innovation Systems & Policy. AIT's shareholders are the Republic of Austria (Federal Ministry for Innovation, Mobility and Infrastructure – BMIMI), which holds 50.46% of the shares, and the Association for the Promotion of Research and Innovation (Federation of Austrian Industries) with 49.54% of the shares.

Center for Digital Safety & Security

At the Center for Digital Safety & Security, more than 230 experts are developing cutting-edge information and communication technologies to ensure that we are able to develop and use these in the context of comprehensive digitalisation and global interconnection in a highly secure and reliable manner.

With its focus on key technology areas such as cyber security, data science and artificial intelligence (AI), quantum and photonics technologies, software for safety-critical systems, digital crisis and disaster management systems, secure software and smart sensor systems, as well as highly reliable next-generation wireless systems, the Center already today makes significant contributions to national and European digitalisation strategies. This technological expertise is complemented by specialised industrialisation expertise, which supports the transfer of innovative research findings into marketable solutions. In these key digital technology sectors, AIT has achieved a successful international leadership position. It thus plays a key role in supporting the EU's objective of ensuring a high level of digital sovereignty in Europe and acts today as a major driver for the positive development of a national digitalisation ecosystem in Austria.

On this basis, the Center for Digital Safety & Security addresses various markets, including the semiconductor industry; the automotive sector; operators of critical infrastructures such as energy grids and power plants; financial markets; the security sector in the context of critical infrastructure protection; as well

as environmental monitoring and crisis and disaster management. In close cooperation with business and industry, academia and the public sector, strategic technology research is carried out, ranging from the development of prototypes to the validation of applications.

Within the national security research community, the Center for Digital Safety & Security holds a recognised position as the most important stakeholder and driving force behind the implementation of the national research strategy for digital security in the national programmes KIRAS, K-PASS and FORTE, bringing together public authorities, industry, SMEs, research and the social sciences to strengthen the competitiveness of Austrian organisations for activities within the EU ecosystem. In the international security research context, the Center has achieved a leading role in comparison with other EU RTOs (Research and Technology Organisations) and has secured a top position in rankings regarding successful EU projects, thereby making a significant contribution to ensuring that Austria, as a high-tech industrial location, has also achieved substantial visibility at international level through cooperation with national authorities such as the Federal Ministry of Defence (BMLV), the Federal Ministry of the Interior (BMI) and the Federal Ministry for European and International Affairs (BMEIA), thereby achieving significant visibility at the international level.

To act as an integral part of an international innovation ecosystem in the field of digital security research, the Center has successfully



established a global dialogue forum in Vienna: the International Digital Security Forum (IDSF). The IDSF is a key flagship conference, developed in close cooperation with Austrian authorities such as the Federal Ministry for European and International Affairs (BMEIA), the Federal Chancellery (BKA), the Federal Ministry of the Interior (BMI) and the Federal Ministry of Defence (BMLV) as well as the Austrian Federal Economic Chamber (WKÖ) and the Competence Center Secure Austria (KSÖ), and which gives Austrian providers and small and medium-sized enterprises (SMEs) in the digital security sector the opportunity to present themselves to an international market. Furthermore, the Center has founded the internationally oriented “PeaceTech Alliance” to promote global multidisciplinary discourse and the development of governance structures for critical digitalisation developments.

With its Center for Digital Safety & Security, AIT is today recognised as a globally accepted brand for digital security competence. The Center cooperates closely, e.g. with the International Atomic Energy Agency (IAEA), the World Institute for Nuclear Security (WINS), the Vienna Center for Disarmament and Non Proliferation (VCDNP), and the UN Office of Counter-Terrorism (UNOCT).

To support data sovereignty objectives in the EU and to promote the development of a new data-driven ecosystem, the Center – jointly commissioned by the Federal Ministry for Innovation, Mobility and Infrastructure (BMIMI) and the State Secretariat for Digitalisation in the Federal Chancellery (BKA) – has also successfully and

significantly driven forward the Gaia-X Hub Austria to accelerate European data ecosystems for economic, environmental and societal value creation. Thanks to the unique design of the national hub, which is based on broad engagement with numerous stakeholders in Austria, and the strategy pursued, the Center has successfully positioned AIT as an EU best-practice example for building EU-wide data technology expertise. Creating federated data spaces is an important foundation for implementing data-driven business models in all relevant markets in industry and the public sector.

The following pages provide a concise overview of the key research and development topics and present selected technological expertise as well as solutions and initiatives developed in the Center. They demonstrate how applied research at AIT, in collaboration with partners from industry, government and society, creates tangible added value, ranging from strategic technology development via prototyping all the way to practical validation. The aim is to provide clients and stakeholders with a clear picture of how the Center for Digital Safety & Security at the AIT Austrian Institute of Technology can support them in addressing current and future challenges in the fields of digital safety, resilience, and technological, data-driven and digital sovereignty.



Contents

4	Preface
6	Introduction
10	1. Cyber Security
11	Cyber Threat Intelligence & AI-Powered Protection
12	Open Source Intelligence (OSINT) Tool “Taranis AI”
12	Machine-Learning-Based Intrusion Detection with “AECID”
12	Systematic Effectiveness Testing of Detection Systems using “Stealth-Cup”
13	Safety & Security by Design
14	Cyber Security by Design Tool “ThreatGet”
15	Post-Quantum Cryptography
16	Certified Services
16	AIT Cyber Range – Training Center
17	Penetration Testing & Red Teaming
17	Security Consulting
18	2. Data Science & Artificial Intelligence
19	Combating Disinformation and Fraud
20	AIT Media Intelligence Plattform
20	DisDETECT – Platform for the Detection and Analysis of Disinformation
20	Fake-Shop Detector
21	Knowledge Management
22	3. Digital Identity Management
23	Biometric Sensor Solutions
23	Face-Snap – Mobile Capture of Biometric Facial Profiles
23	Touchless Four Fingerprint (T4F) Scanner

24	4. Protecting Critical Infrastructures	43	9. International Network
25	fiberRAIL® – Distributed Acoustic Sensing (DAS)		
26	Optical Sensor Technology – FrontierSense	45	10. Selected Research Infrastructures
27	5. Crisis and Disaster Management	46	Photonics & Quantum Communication Laboratory
28	Situational Awareness & CBRNe	46	Radio Frequency Laboratory
29	Horus3D Software Platform	47	AIT Cyber Range – Test & Training Center
29	RaptoR Software Module	48	11. Certifications
29	MuFASA Software Framework		
30	6. Sustainable & Resilient Society	49	Imprint
31	Digital Solutions for Protecting the Environment		
32	AIRDB – Intelligent Solution for Air Quality Measurement		
32	EMIKAT – Comprehensive Solution for the Management and Analysis of Emission Data		
33	Smart Cities & Municipalities		
33	Data Exchange		
33	Knowledge Management		
34	Marketplace		
34	Reporting & Digital Twin		
35	7. Enabling Digital Technologies		
36	Next-Generation Chip Technologies		
37	Quantum Encryption		
38	Next-Generation Wireless Technologies		
39	8. Initiatives and Platforms		
40	Gaia-X Hub Austria		
41	International Digital Security Forum (IDSF)		
42	PeaceTech Alliance		

1 CYBER SECURITY

As a national competence center for cyber security and an international contact point for training and education, as well as for state-of-the-art digital tools for cyber security, the AIT Center for Digital Safety & Security has decades of experience in protecting control systems in critical infrastructures, and it now operates the specialised, hybrid and flexibly adaptable IT simulation environment "AIT Cyber Range", where international cyber security training courses are conducted. In combination with the development of cutting-edge tools and methods that follow the "Security & Privacy by Design" approach, the experts are committed to the highest standards of computer security and prioritise the responsible use of technology over purely technical or economic objectives. Furthermore, the Center provides significant support for the objectives of the national cyber security strategy through new solutions and the development of capabilities.

Cyber Security

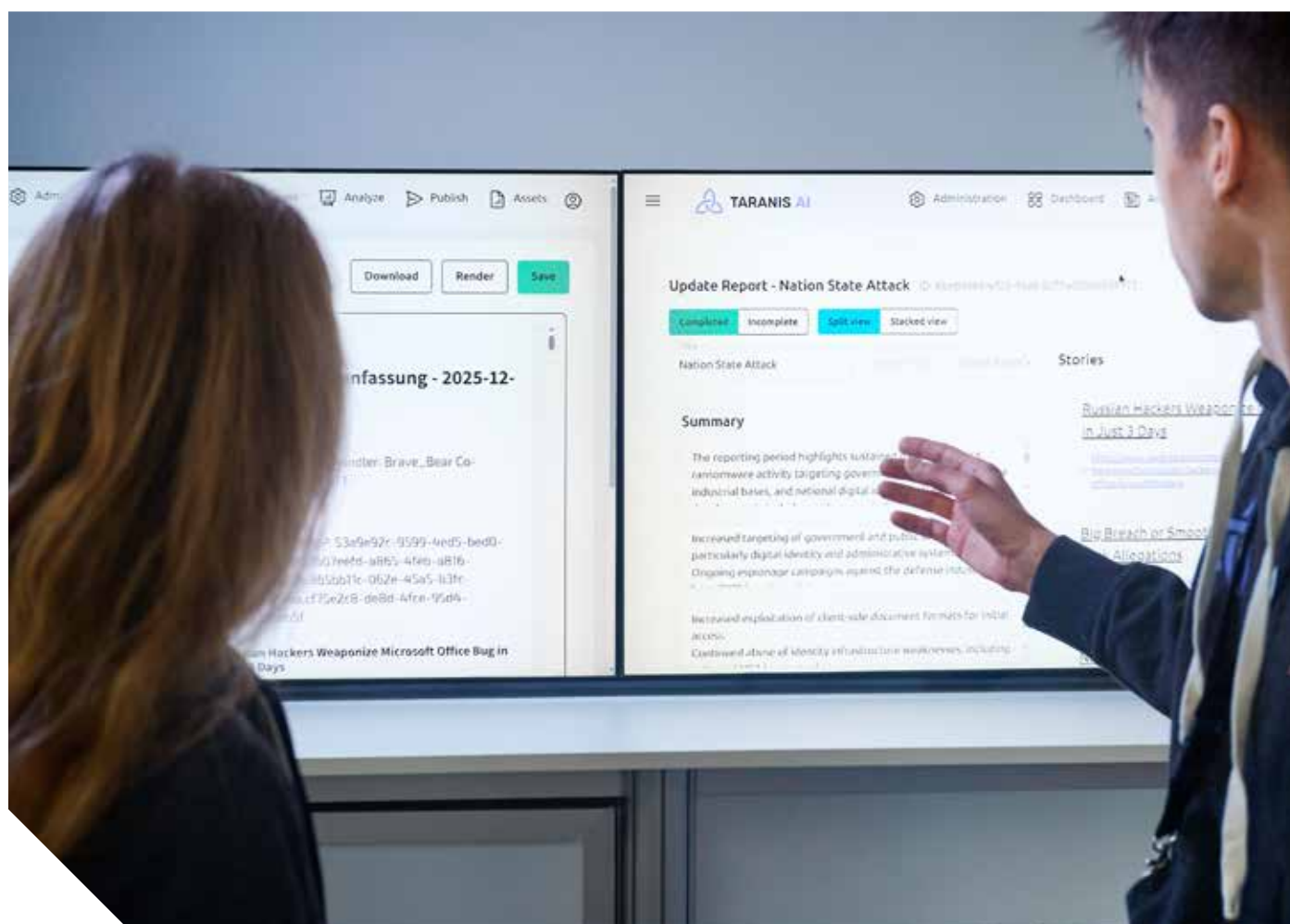


Cyber Threat Intelligence & AI-Powered Protection

Every day, companies and organisations are exposed to dangerous cyberattacks. In the fight against these threats, data security experts must constantly monitor the respective situation, define key indicators, respond promptly to problems and stay up to date with the latest attack vectors, methods and threats. However, managing to do all this at once is often a daunting task.

The Center is working on novel intrusion detection systems (IDS) that use machine learning to characterise system behaviour and detect deviations from a defined baseline. With the help of these solutions for the adaptive processing of network log streams, frequently occurring patterns in log files can be identified, classified and clustered, ultimately distinguishing known normal activities from unknown malicious activities within corporate IT infrastructures – a self-learning approach requiring minimal manual configuration.

By effectively integrating with threat detection solutions, the anomaly detection system can be customised and focused on specific threat areas. Conversely, by extracting indicators from raw log data, information about potential threats can be obtained with minimal staff involvement.





Taranis AI



Open Source Intelligence (OSINT) Tool „Taranis AI“

Taranis AI is an advanced open-source intelligence tool (OSINT) that uses artificial intelligence to revolutionise information gathering and situation analysis. It offers powerful OSINT capabilities for the automated analysis of large volumes of unstructured news sources.

Using artificial intelligence and natural language processing, relevant content is collected from various data sources, enriched and processed to ensure high quality. An analyst-friendly workflow environment enables raw information to be efficiently converted into structured reports and to create tailored end products, such as structured reports or PDF dossiers. This is complemented by seamless publication features and experimental options for collaborative threat intelligence work, such as story-level sharing via MISP (Malware Information Sharing Platform), an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats.



AECID



Machine-Learning-based Intrusion Detection with „AECID“

The abbreviation AECID stands for “Automatic Event Correlation for Incident Detection” and refers to a machine-learning-based method for the automatic detection of security incidents. Through the continuous analysis of system events in log data and the application of specialised mathematical methods, AECID can distinguish normal from anomalous behaviour in complex computer networks.

Unlike conventional approaches, the algorithm does not require detailed prior knowledge of the IT systems to be monitored. Instead, following a learning and observation phase, AECID independently recognises patterns in system behaviour. This is based on a self-learning algorithm that identifies typical processes and automatically detects deviations.

The AECID technology developed at AIT continuously adapts to new situations and does not require time-consuming system modelling or complex configuration management by the operator. By continuously recording and analysing new information, AECID constantly expands and refines its knowledge base, gaining ever more precise insights into the respective system in use.



Stealth-Cup



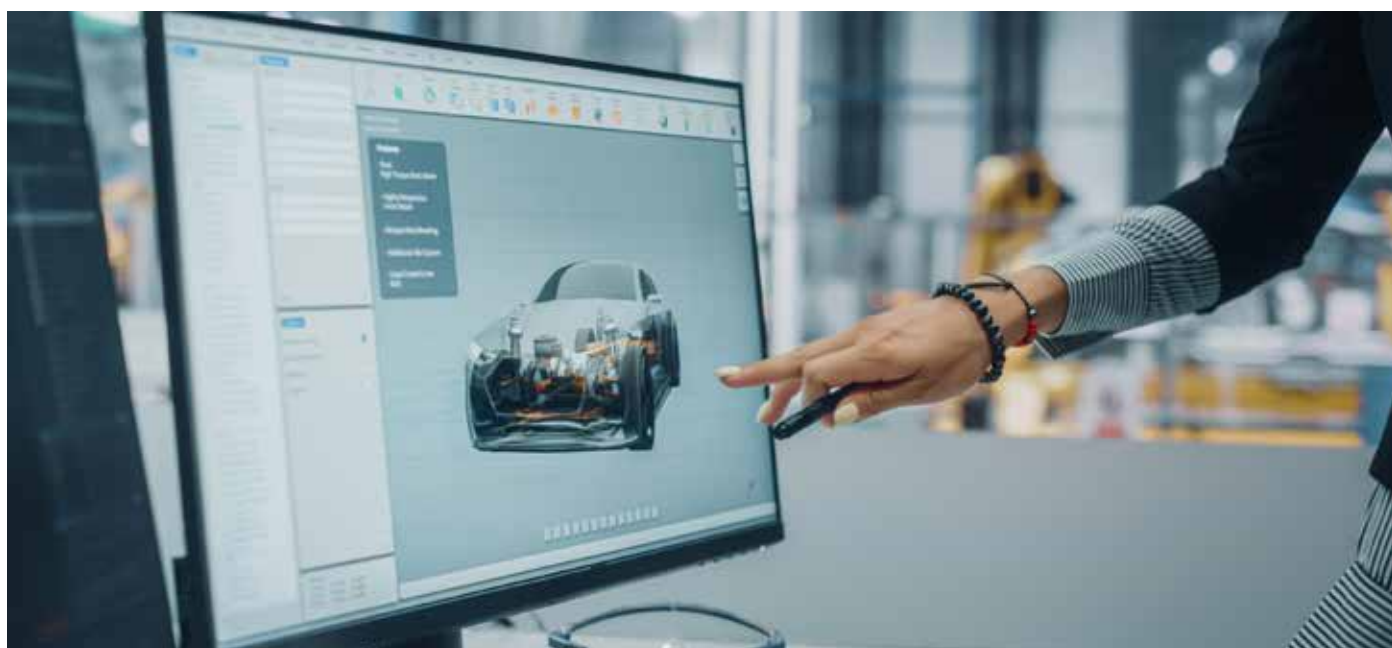
Systematic Effectiveness Testing of Detection Systems using “Stealth-Cup”

Intrusion detection systems (IDS) are key components of modern cyber security protection, detecting attacks in modern computer networks. Nevertheless, their actual effectiveness, particularly under real operating conditions, remains difficult to measure. The “Stealth-Cup” methodology is a research and evaluation concept developed at AIT that is unique internationally; it enables realistic, multi-stage cyber attacks in a fully automated IT/OT cyber range. This approach lays the foundation for realistic and reproducible assessments of intrusion detection systems (IDS) in large IT/OT systems.

AIT's leading role in the field of realistic IDS evaluation is evident from several clear indicators. The infrastructure has been developed and validated in collaboration with infrastructure companies, demonstrating its relevance and practical applicability. The “Stealth-Cup” offers a combination, unique in Europe, of a fully reproducible “Infrastructure as Code (IaC)”-based test environment and realistic attack patterns generated by human attackers. By providing independent, scientifically robust evaluation and testing capabilities, AIT is supporting Europe's competence to assess security-critical technologies in a transparent and evidence-based manner, thereby helping to strengthen Europe's capacity to evaluate modern detection systems in a realistic manner and to build robust defence mechanisms. “Stealth-Cup” is aimed at European authorities, organisations and manufacturers, particularly in the fields of detection engineering and staff training.

Safety & Security by Design

With the increasing digitalisation of industrial processes, there is a growing need for secure development approaches to minimise vulnerabilities right from the inception of IT/OT systems and to strengthen companies' competitiveness. This is because traditional security measures usually only come into play after IT/OT systems have been developed, leaving potential vulnerabilities undetected and increasing the risk of cyberattacks. Hence, industrial companies in particular need effective methods to identify and close security gaps at an early stage. At the same time, international standards must be adhered to in order to secure competitiveness in the global market.



These requirements are becoming even more important as modern digital systems increasingly operate autonomously and are based on artificial intelligence – e.g. in industrial automation, in networked production facilities or in safety-critical applications. AI-supported systems are making decisions increasingly independently and in real time. This not only increases efficiency and performance, but also the demands on reliability, traceability and controllable system behaviour. Unintended or undesirable reactions from such systems can have significant safety, economic and legal consequences.

Against this backdrop, the Center for Digital Safety & Security at AIT has specifically built up expertise in “Safety & Security by Design” to complement its established cyber security expertise. The aim is to systematically integrate safety and reliability requirements into the development process of digital and AI-based systems from the outset, rather than testing them retrospectively. A particular focus is placed on methods that are also capable of handling the complexity, uncertainty and adaptability of modern AI systems.

To this end, the Center's experts are developing and testing structured development, testing and verification approaches that enable

end-to-end quality assurance throughout the entire lifecycle of digital systems, from concept via operation all the way to further development. In doing so, the operational limits and operating conditions (Operational Design Domains) are also clearly defined to ensure that systems operate only within the parameters for which they were designed and tested.

On this basis, the experts have developed ThreatGet, an innovative “security-by-design” development technique, which is an internationally recognised method that supports companies in implementing security requirements at an early stage, systematically and in compliance with standards. The Center's specialists also play a leading role in international standardisation (IEC, ISO) and thus actively contribute to the further development of regulatory frameworks, e.g. in connection with the Cyber Resilience Act. In this way, the AIT Center makes a significant contribution to the secure introduction of complex digital and AI-based systems and to sustainably strengthening the competitiveness of Austrian industrial companies.

Dependable
Systems
Engineering





ThreatGet



Cyber Security by Design Tool “ThreatGet”

The award-winning ThreatGet security tool, which is based on artificial intelligence, enables the analysis of the entire system architecture of safety- and security-critical applications, such as connected vehicles. The automated analysis of potential system risks and attack vectors can be carried out seamlessly right from the start of system development. This “Cyber Security by Design” tool is a must-have for industries with safety- and security-critical

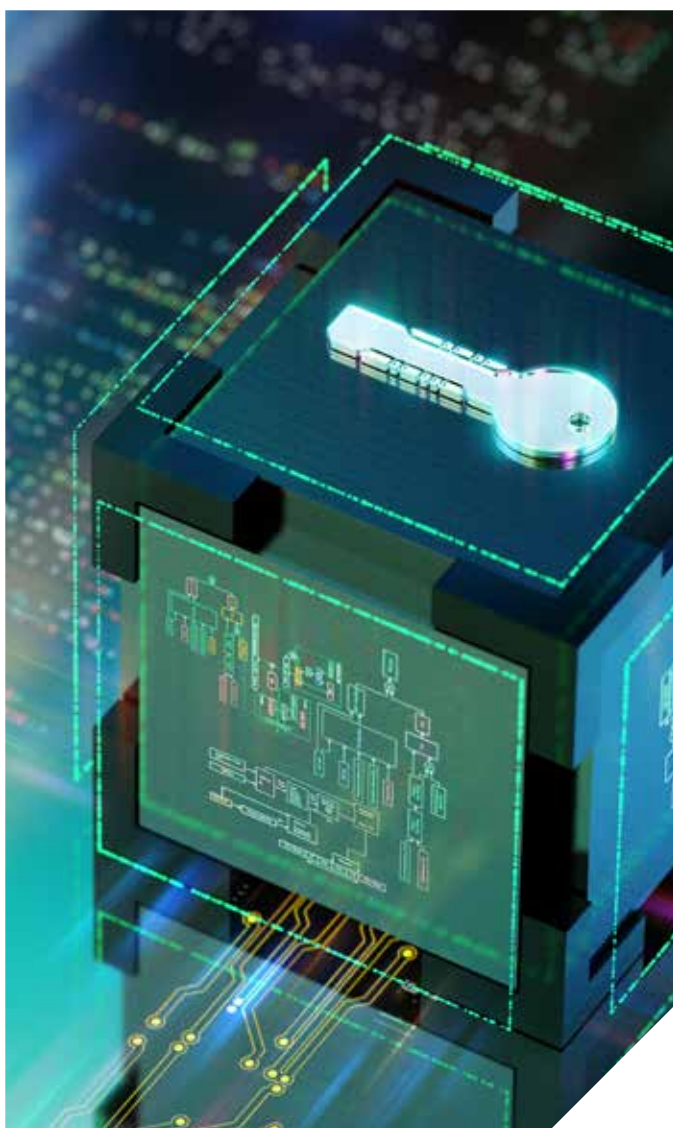
infrastructure that are required by law to establish a suitable cyber security management system. ThreatGet received the Constantinus Award in the “Digitalisation/IoT” category in 2021 and was nominated for the “Austrian State Prize for Consultancy” in the “Management Consultancy and IT” category in 2022.



Post-Quantum Cryptography

The ongoing development of cryptographically relevant quantum computers is creating a need for methods that can guarantee the integrity, authenticity and confidentiality of data in the long term and in a verifiable manner, even in a “post-quantum” world.

“Quantum computer safe” technologies are encryption methods that cannot be decrypted by quantum computers, even once they become available.



In recent years, the Cryptography Group at the Center for Digital Safety & Security at AIT established a corresponding research focus to position AIT as a competence center for post-quantum secure cryptography (PQC) within Austria, as well as in a European and international context. The group is developing methods that will continue to provide verifiable security guarantees for data with powerful quantum computers in a “post-quantum world”. In close collaboration with the Center's experts in quantum encryption, the team is working on hybridising post-quantum secure methods with quantum key distribution (QKD) in order to combine the physical security guarantees of QKD with the end-to-end security guarantees of PQC. Parallel to this, the expertise gained at all levels is actively contributed to European and international standardisation efforts.

As coordinator of projects such as PREPARED (KIRAS), AUTKRYPTO (K-PASS) or QCI-CAT (Digital Europe Programme) as well as a partner in projects such as POSEIDON (Horizon Europe), the team has established itself as a reliable partner and central point of contact for post-quantum research for Austrian stakeholders and beyond. A case in point: the migration of existing complex systems was demonstrated as part of the KIRAS project PREPARED, in which – together with the Federal Chancellery and other partners from industry and academia – ID Austria's PDF signature solution was prototypically converted into a post-quantum secure version.

KIRAS



PREPARED



QCI-CAT



POSEIDON

Post-Quantum
Cryptography

Certified Services

Practical cyber security services help organisations strengthen their digital resilience throughout the entire security lifecycle in a sustainable manner. The range of services includes realistic training and simulation environments using the AIT Cyber Range, technical security audits and penetration tests, and strategic security consultancy aimed at safeguarding modern digital systems, processes, and critical infrastructure.

AIT Cyber Range – Training Center

In the context of expanding EU-wide cyber security capabilities and developing specialised professional training programmes for public authorities, critical infrastructure operators and SMEs, AIT, with its Center for Digital Safety & Security, is now recognised internationally as a leading stakeholder. In close cooperation with international partners such as the International Atomic Energy Agency (IAEA), the World Institute for Nuclear Security (WINS), the Vienna Center for Disarmament and Non Proliferation (VCDNP), and the UN Office of Counter-Terrorism (UNOCT), the AIT Center conducts training courses worldwide.

In an age of increasing digital threats and global interconnectedness, securing critical infrastructure is essential to ensuring national and international stability. Cyber security is therefore a key international research area, both for the development of effective defence technologies and for building defence and counter-attack capabilities for organisations, which may also be deployed within state security structures. With growing dependence on digital systems, the risk of cyberattacks on critical infrastructure such as energy supply, healthcare, transport networks or government departments is rising enormously. These attacks can not only cause economic damage but also jeopardise public safety and trust in state institutions. There is an urgent need for practical, innovative training methods to prepare IT security experts, operators of critical infrastructure and Security Operations Centers (SOCs) to detect, analyse and respond to current and future threat scenarios.

At AIT, the Center for Digital Safety & Security has therefore established the AIT Cyber Range, an innovative simulation environment designed to realistically replicate IT and OT networks in safety-critical environments (digital twin). The Cyber Range is used for training in the defence against cyber attacks on critical infrastructure and corporate networks and is offered worldwide in combination with bespoke training programmes for operators of critical infrastructure, public authorities and SMEs. A particular focus is placed on training courses covering the establishment and operation of Security Operations Centers (SOCs), including vulnerability management, threat analysis and the response to cyber incidents under realistic conditions.

Reference clients include the World Institute for Nuclear Security (WINS); the United Nations Office for Counter-Terrorism (UNOCT); the Competence Center Secure Austria (KSÖ); and the Federal Ministry of the Interior (BMI); EU missions; national infrastructure operators such as Wien-IT, and energy network operators such as Verbund, EVN and Salzburg AG. Finally, the experts also collaborate, e.g. through initiatives of the Austrian Federal Economic Chamber (WKO) with Digital Factory Vorarlberg (DFV) as well as with companies in the manufacturing industry and SMEs.

Training programmes accordingly designed to develop specific skills for public authorities and infrastructure operators were implemented, e.g. in Europe (the UK, Slovenia, Romania and Ukraine), in those African countries where French or English is spoken, and in the Arab states of Oman and the United Arab Emirates. Training activities also took place in Asian countries such as Korea, Thailand, the Philippines and Vietnam, as well as in South America. Together with the Federal Ministry for European and International Affairs of the Republic of Austria (BMeiA), the AIT Center for Digital Safety & Security was also one of the key players in the Republic of Austria's signing of the UN Cybercrime Convention in Vietnam, as well as the driving force behind the establishment of cooperation between Vietnam and Austria in the field of cyber security capacity building.



Penetration Testing & Red Teaming

A penetration test, or pentest for short, is an empirical security check carried out under defined conditions. It involves the use of real and/or common tools and techniques that would also be used by potential attackers. Penetration tests provide a snapshot of the tested components from a specific perspective. Generally, the number of vulnerabilities identified increases with the effort expended and the information available about the system being tested.

The majority of penetration tests currently available on the market focus on exploiting already known vulnerabilities. In this case, the testers, who are supported by security software, rely on the automated evaluation of the security level of the test components. The experts at AIT take a different approach, though. The specialists draw on their expertise from a wide range of high-calibre research projects. As a result, the tests also uncover new, previously unknown vulnerabilities (zero-day vulnerabilities).

The Center's team supports clients from the initial prototype right through to final implementation. Whether it involves black-box testing without detailed knowledge of the system under test, or white-box testing where comprehensive information is available, all the way to extensive source code analysis. The experts possess the necessary expertise and many years of project experience.

IT security is a highly sensitive topic, so no references are published. Clients served come from all sectors of business, culture, the media, politics, sports and the public sector. To nevertheless highlight our expertise in this field, some of the security vulnerabilities discovered and reported by our experts are listed here.

Security
Advisories



Further information on the certified services offered by the AIT Center for Digital Safety & Security in the areas of penetration testing, red and purple teaming, and vulnerability scans / security audits can be found here.

Penetration
Testing



Security Consulting

The Center also offers its broad expertise in the field of cyber security as a bespoke consultancy service. Working closely with clients, the experts assess the individual starting situation and discuss current problem areas and future requirements. In the run-up to the consultancy project, manageable modules with a clear focus on results are defined, thereby giving clients the opportunity for independent and sustainable further development within their own organisations. The progress achieved by clients in this way represents a significant step towards a cyber-secure society.

AIT's security consulting services provide organisations with comprehensive support in making their IT secure, resilient and

future-proof. The services range from optimising and redesigning IT and business processes, via establishing effective information security and business continuity management systems, all the way to strategic IT alignment. This also includes audits in accordance with recognised standards and the practical implementation of data protection requirements. The aim is to minimise risks, efficiently meet regulatory requirements and establish IT as a reliable foundation for stable, sustainable business processes.

Security
Consulting



2 DATA SCIENCE & ARTIFICIAL INTELLIGENCE

In the field of Data Science & AI, a team of around 50 experts at AIT's Center for Digital Safety & Security develops human-centred, trustworthy and explainable AI solutions that specifically address social, economic and security-relevant challenges. The focus is on responsibly designed applied AI that creates genuine added value. This ranges from providing data-driven bases for decision-making for public authorities and businesses, via protecting consumers and democratic decision-making processes, all the way to safeguarding critical infrastructures. AIT's AI systems are designed to analyse complex unstructured data from images, videos, audio and text sources, as well as sensor data, and to derive predictions about future developments.

One central research element is the explainability and traceability of AI decisions, which is regarded as a crucial success factor for building trust, acceptance and regulatory compliance. By closely integrating data science, cutting-edge AI methods and ethical guiding principles, the AIT Center helps to strengthen digital sovereignty and to implement innovations in a sustainable, traceable and socially effective manner.

Furthermore, the Center consistently pursues a vertical AI approach, combining in-depth domain expertise with cutting-edge AI methods. The aim is to develop tailor-made solutions for a range of application areas, from specialised technical applications all the way to complex, cross-sector systems. The Center's expertise is deliberately designed to span technologies and industries, enabling it to address diverse AI challenges in a well-founded, responsible and practical manner.

Data Science & AI



Combating Disinformation

The experts develop algorithms and technologies for the analysis, interpretation and comprehensible presentation of multimedia content such as images, videos, audio files and texts. Using modern computer vision methods, objects, faces and patterns in media content are automatically recognised, classified and assessed for authenticity.

In addition, Natural Language Processing (NLP) and Explainable AI (XAI) are used to analyse text-based content such as subtitles, social media posts, comments or metadata, and to make judgments regarding plausibility, origin and possible manipulation. By combining visual and language-based analysis methods, multimodal disinformation can be reliably detected, explained in a comprehensible manner and contextualised.

In addition, context enrichment methods enable media content to be cross-referenced with additional information such as location, time or sources. The modular and scalable design of these methods allows for the efficient processing of large volumes of data and supports applications in digital forensics, the fight against disinformation, the OSINT (Open Source Intelligence) environment, and security-critical analyses by law enforcement and security agencies.





AIT Media Intelligence Plattform

The AIT Media Intelligence Platform is an AI-powered, modular analysis ecosystem for the forensic examination of digital media content. It supports human experts in identifying disinformation, manipulation and content that threatens democracy, offering authorities, organisations and companies powerful tools for fact-checking, media verification and situational analysis. The platform combines digital multimedia forensics, context enrichment and explainable AI to efficiently analyse large volumes of text, image, audio and video data and place them in a comprehensible context. The modular structure allows for the targeted use of specialised analysis tools that can be flexibly combined and operated on a scalable basis.

Key functions include the detection of deepfake videos and speech, synthetic faces, face morphing, AI-generated images as well as manipulated media content. This is complemented by natural language processing for analysing hate speech, extremism, propaganda, conspiracy theories, discrimination and toxic language. Furthermore, the platform supports knowledge extraction through text and sentiment analysis, style and writing pattern recognition, image and video search, object and symbol recognition, and image geolocation.

The AIT Media Intelligence Platform delivers real-time results, supports collaborative working and, as a continuously evolving solution, is available both online and via bespoke implementations and integrations. It thus enables the identification, understanding and contextualisation of complex media content, providing a basis for informed decisions in fields relevant to security, society and democracy.

DisDETECT – Platform for the Detection and Analysis of Disinformation



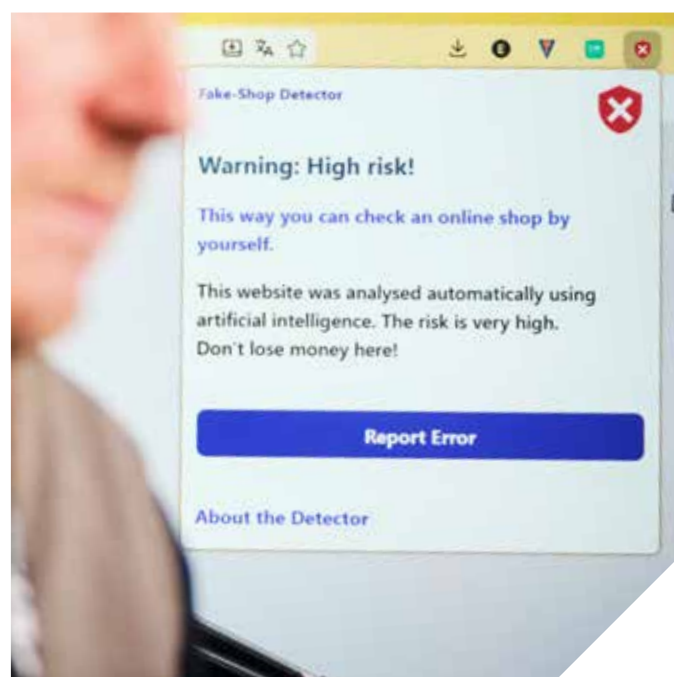
DisDETECT is a system for the semi-automatic detection and analysis of disinformation and related phenomena such as hate speech, toxic language and propaganda in German-language online media. It combines narrative, argumentative and framing-related features with transformer models, linguistic features and knowledge graph embeddings to reliably capture different forms of communication. The results are presented in a web-based application with interactive visualisations, serving as a basis for subsequent analysis by experts.



Fake-Shop Detector

Fake online shops are becoming more numerous and, at the same time, harder to spot. The Fake-Shop Detector, developed by the AIT Center in close cooperation with the Austrian Institute for Applied Telecommunications (ÖIAT) and the Austrian IT specialist X-Net, offers support in tracking down online fraudsters. The Fake Shop Detector checks unknown online shops for more than 21,000 features in real time using artificial intelligence. In particular the permanent quality control of the artificial intelligence by human beings is an inherent part of the AI-based solution.

If a shop is suspicious, the Detector issues a warning and proactively protects consumers from online fraud. This success of the Fake-Shop Detector has led to a partnership between AIT and the Bavarian Ministry of Justice. The aim of this partnership is to adapt the Detector to the specific requirements of law enforcement agencies and to further develop it for their investigations. Furthermore, this tool has won multiple awards (eAward 2023, State Prize for Digitalisation 2024, Constantinus Award 2024, KSÖ Security Prize 2024) and was most recently the Austrian winner among 35 international cyber security products tested for their effectiveness against fake shops by the independent system testing expert "AV-Comparatives". The development of the Fake-Shop Detector was funded by the Austrian Federal Ministry of Finance as part of the KIRAS security research programme.



Knowledge Management

In the field of Knowledge Management, the AIT Center develops methods for the efficient indexing and utilisation of large, heterogeneous datasets. The work builds on more than two decades of research into providing access to digital cultural assets based on the “FAIR” principles (Findable, Accessible, Interoperable, Reusable), including in collaboration with the European cultural heritage portal Europeana.

The focus is on multimodal information retrieval, in which different data types – such as text, images or structured data – are analysed together and linked with each other. Through cross-modal search methods (e.g. text-to-image or image-to-text) and user-friendly presentation of the results, relevant information can be efficiently found within large datasets and organised into curated collections.

Semantic and embedding-based indexing methods are used, as well as large language models that enable natural language queries across heterogeneous data sources. The aim is to transform existing information resources into rich semantic structures such as knowledge graphs, thereby sustainably improving their use for analysis, research and decision-making processes.



Europeana



Knowledge Management



3 DIGITAL IDENTITY MANAGEMENT

The AIT Center for Digital Safety & Security develops cutting-edge technologies for the rapid, accurate and secure identification and verification of identities. These innovations set new standards in terms of security, convenience and data protection. They are as an international success story for the responsible digitalisation of security-critical applications. The foundation for this is the Federal Ministry of Finance's (BMF) national security research programme KIRAS, in close collaboration with the Federal Ministry of the Interior (BMI) as the end user and an international pioneer in the security sector. Together with AIT's technological research and development excellence, this collaboration positions Austria as an international model for the responsible digitalisation of sensitive data, thereby making a decisive contribution to Europe's digital sovereignty.

With the increasing digitalisation of services and the growing importance of secure authentication methods, there is a rising demand for innovative, reliable and user-friendly technologies for digital identities and biometric security systems. Traditional biometric systems, such as contact-based fingerprint sensors in security-critical areas like airports, are increasingly reaching their limits. Contact-based systems are susceptible to tampering, they are unhygienic and often not user-friendly. Parallel to this, automated, trustworthy video analysis and sensor systems operating across different optical spectra are gaining in importance, for instance in the protection of critical infrastructures, public spaces or strategic facilities.

At the same time, there is a growing need for responsibly designed, secure and data-protection-compliant solutions that meet both user requirements and strict security standards. As part of its digital sovereignty strategy, the EU aims to develop and deploy such technologies independently and securely within its jurisdiction. Organisations such as the United Nations (UN) also support the global community of nations in establishing secure system solutions and ensuring the responsible handling of sensitive biometric data.

Computer Vision



Biometric Sensor Solutions

In the field of technologies for the verification of digital identities and in modern biometric sensor technology, AIT, with its Center for Digital Safety & Security, is regarded as an important international technology leader in contactless – and therefore secure, hygienic and user-friendly – fingerprint sensor technology for biometric authentication.

The institution thus makes a significant contribution to the EU's digital sovereignty as well as to the global security infrastructure. Through this "Made in Austria" technological development, AIT is making a significant contribution to the EU's digital sovereignty objectives today.

AIT's leading role in the field of contactless fingerprint sensor technology is impressively demonstrated through international licensing agreements with providers such as T3K and a global airport security company, a certification partnership with the German Federal Office

for Information Security (BSI), and collaboration with the UN Office for Counter Terrorism (UNOCT) on the www.responsible-biometrics.org platform.

Responsible
Biometrics



In addition, concrete technology implementation projects are already underway with industry partners and authorities within the EU in the sense of a responsible roll-out phase, such as the deployment of the new fingerprint sensor technology by the Austrian police. Cooperation with the UN in a global context is also planned for these future-oriented digital technologies.

Face-Snap – Mobile Capture of Biometric Facial Profiles

In the context of digital identity solutions, the Center for Digital Safety & Security is developing innovative applications for mobile biometric capture. Face-Snap enables the rapid and secure creation of facial profiles directly via a smartphone, thereby supporting emergency services in carrying out their daily work efficiently.

The application allows high-quality facial images to be captured directly in the field and processed immediately. This significantly simplifies the previously time-consuming process of facial capture, saving time and improving the efficiency of investigation and identification processes.

Face-Snap also integrates automated quality checks based on international ICAO standards. The application alerts users when images need to be optimised to ensure the best possible image quality. This ensures that only suitable and standard-compliant images are included in biometric databases.

The solution was developed in close collaboration with police authorities to ensure that legal, operational and security-related requirements were taken into account from the outset. Face-Snap supports authorities in streamlining their processes while meeting high standards of data protection and security. Face-Snap is an important component of modern digital identity solutions in the security sector.

Touchless Four Fingerprint (T4F) Scanner

T4F



The Touchless Four Fingerprint (T4F) Scanner uses camera-based capture to enable the contactless capture of four fingerprints simultaneously. This solution meets the highest requirements on hygiene, security and user comfort, and is particularly suitable for access control, border control and secure authentication processes. Contactless capture prevents latent fingerprints, makes attempts at deception more difficult and, at the same time, ensures compatible use of existing fingerprint databases without the need for adjustments to downstream verification or authentication systems.



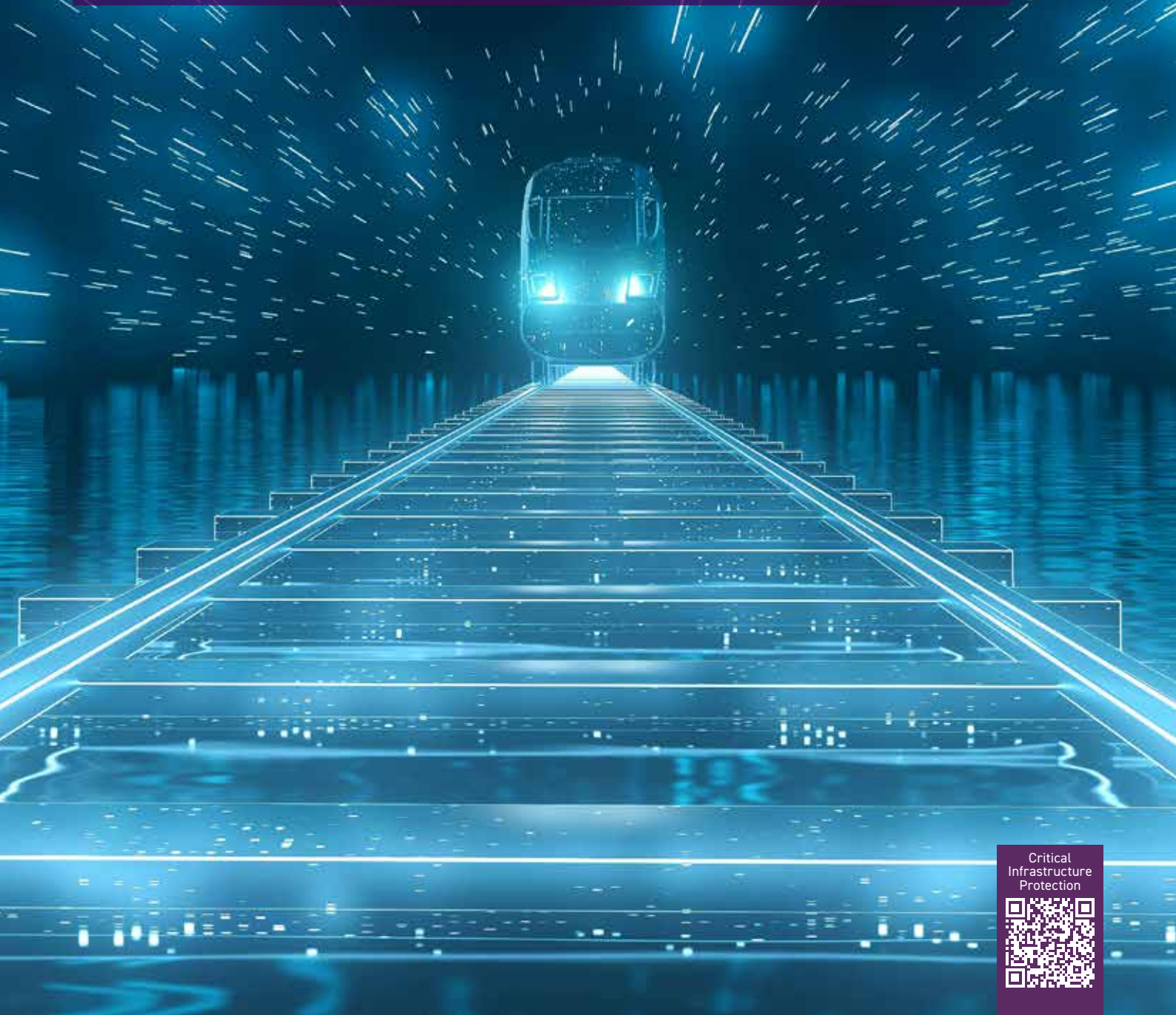
Biometric Sensor
Technology



4 PROTECTING CRITICAL INFRASTRUCTURES

Modern societies rely on efficient and secure infrastructure. At the same time, the demands placed on their availability, resilience and security are increasing. Therefore, operators of critical infrastructure need new approaches to continuously monitor the condition of their systems, detect potential disruptions early and minimise risks effectively. AIT is developing intelligent monitoring and analysis methods for this purpose. To this end, the experts combine modern sensor technologies, data-driven analyses and operational decision support. This creates transparency regarding the condition of plants and networks, enabling resilient operational processes.

A key area of expertise is Distributed Acoustic Sensing (DAS). This involves using existing fibre-optic infrastructure as a large-scale, continuous sensor network. This enables events along the infrastructure to be detected and analysed. Additionally, AIT enhances the protection of critical infrastructure through optical sensor technology and video analysis across different spectral ranges. These technologies support public safety stakeholders in reliably and efficiently evaluating visual information. By combining distributed acoustic and optical sensor technology with AI-supported interpretation and operational information processing, AIT creates solutions that enable security organisations, infrastructure operators and public authorities to identify critical situations earlier, gain a better understanding of complex environments and act in a more coordinated manner.



Critical
Infrastructure
Protection



fiberRAIL® – Distributed Acoustic Sensing (DAS)

fiberRAIL®



Critical infrastructures such as rail networks, roads, and energy and communication lines span vast distances and require continuous monitoring. Traditional surveillance solutions rely on point sensors or cameras that cover only limited areas, that incur high installation and maintenance costs, and that are difficult to scale. At the same time, demands for security, availability and efficiency are rising – particularly in transport and for safety-critical facilities. Distributed Acoustic Sensing (DAS) offers the basic potential to bridge this gap. DAS can, for example, provide an ideal complement to train positioning, since – unlike GNSS (Global Navigation Satellite System) – it is under the full control of the rail infrastructure operator in terms of infrastructure, it determines positions in real time with high accuracy, and it simultaneously localises both the front and rear of the train.

The AIT Center plays a leading role at the interface between DAS technology, AI-based analysis and safety-critical applications.

fiberRAIL® is an innovative, fibre-optic-based track-and-monitor system developed at AIT that supports railway infrastructure operators in monitoring trains and track systems in real time, without the need for additional hardware on vehicles or expensive sensors on the track. By utilising existing fibre-optic cables along the route, the solution provides continuous information on train position, speed, length and direction of movement, thereby enabling precise, seamless tracking of all train movements.

At the same time, fiberRAIL® detects safety-critical events such as broken rails, wheel damage, derailments or lost carriages at an early stage and reports all incidents in real time. The platform furthermore supports predictive maintenance and ensures the safety of workers along the tracks. At the same time, it provides documentation on control systems and, consequently, train behaviour to minimize infrastructure wear and tear. fiberRAIL® is modular, low-maintenance and enhances both safety and efficiency in railway operations.



FrontierSense



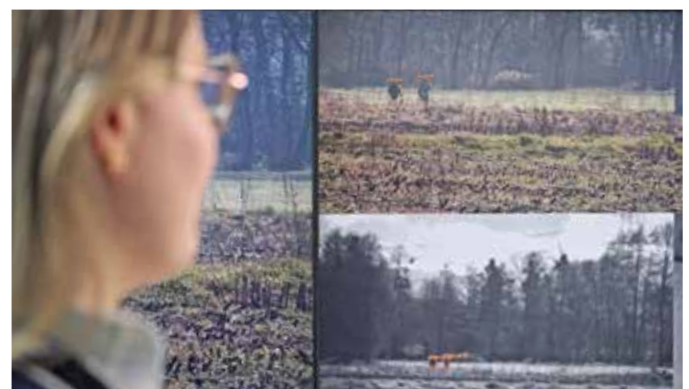
Optical Sensor Technology – FrontierSense

AIT's research focus in the field of optical sensor technology supports key industrial and government stakeholders in the area of public security by providing supportive video analytics technologies. The Center's experts are working on trustworthy, automated, user-friendly and innovative solutions that can be used for video analysis across various optical spectra, for example at land and sea border crossings. The target audience includes stakeholders involved in the protection of critical infrastructures (borders, power stations, transport hubs, etc.), public spaces (event venues, festivals, etc.), as well as remote areas (e.g. oil fields) or the defence sector.

FrontierSense is a ready-to-use multisensor platform featuring edge AI, designed as a compact, modular solution that can be deployed in operational frontier environments. Designed for critical and resource-constrained environments, the FrontierSense platform integrates heterogeneous sensors with tried-and-tested, on-device AI analytics to automatically detect, interpret, and contextualise objects, events or the environment in real time – delivering decision support precisely where it matters most. Diverse, heterogeneous sensors provide robust, analysis-ready data that remains interpretable and reliable even in adverse weather and complex environments.

Built on an interoperable and modular architecture, FrontierSense combines robust multi-sensor data capturing (FrontierSense Core) with advanced edge-based AI and analytics (FrontierSense Insight), thus enabling scalable deployment across safety and security-relevant domains and critical infrastructures. By processing data locally at the edge, FrontierSense reduces latency, preserves data sovereignty, and supports resilient operations even under limited connectivity.

FrontierSense empowers operators and authorities with timely, actionable insights – enhancing situational awareness, supporting informed decision-making and strengthening operational resilience on any frontier.



Optical Sensing



5 CRISIS AND DISASTER MANAGEMENT

In dynamic and security-critical environments, having an up-to-date and reliable situational overview is essential for effective coordination and informed decision-making. Public authorities, emergency services, and critical infrastructure operators must consolidate and evaluate information from a variety of sources, translating it into concrete actions within a short timeframe. AIT therefore develops systems for situation assessment and decision support. These systems integrate heterogeneous data sources, sensor information, geodata and operational processes to provide a unified situational picture. In this way, AIT experts help organisations better understand complex situations, identify risks early on and make coordinated decisions in real time.

By providing these solutions, AIT is helping to sustainably improve crisis response, disaster management and societal resilience. The aim is to provide emergency services and public authorities with reliable, practical, technologically advanced systems.

Crisis &
Disaster
Management



Situational Awareness & CBRNe

Providing optimised decision-making bases is a key requirement for crisis and disaster management. The focus is on digital platforms and system solutions that enable interoperable and secure communication, shared situational awareness, and coordinated decision-making among emergency services, authorities and operators of critical infrastructures.

In an increasingly complex global security landscape, the ability to detect and respond to chemical, biological, radiological, nuclear and explosive (CBRNe) threats is more important than ever. Advances in surveillance technology and situational awareness systems are shaping the future of defence and emergency response. They enable faster and more precise identification and management of threats. The combination of cutting-edge research and international co-operation is yielding innovative solutions to improve security for the armed forces, civil protection agencies and the general public. Against this backdrop, the European Commission's CBRNe Action Plan also highlights the need for the EU to strengthen its resilience and improve its preparedness for dealing with CBRNe threats.

Over the past 15 years, the AIT Center for Digital Safety & Security has built up comprehensive expertise in the field of sensor technologies for situational awareness and analysis through numerous projects within Austrian security research programmes (KIRAS and Forte) as well as European security research programmes (FP7, H2020, Horizon Europe). With the know-how gained in developing CBRNe risk awareness and protecting civilian and military

forces in crisis and emergency situations, AIT has also taken on a leading role in initiatives under European defence programmes.

A central component of digital CBRNe defence is the development of modular system-of-systems architectures that combine sensors, platforms and software components into an integrated overall system. In this context, new functional software components for situational awareness have been developed, and a multinational integration concept for CBRNe reconnaissance and surveillance systems was defined. This architecture provides the basis for the flexible integration of existing and future technologies.

In the field of decision support for crisis and disaster management, the Center has developed methods for the optimised selection and objective evaluation of solutions, as well as for validating the impact of measures. To improve cooperation between stakeholders, the use of data rooms in crisis and disaster management is also being promoted. Use cases are connected with resource management, enabling improved, cross-organisational deployment of volunteers and ensuring resilient supply chains in crisis situations.



Horus3D Software Platform

The Horus3D software platform is a key technological component for the analysis of complex environments. It processes sensor data from various platforms and uses it to generate detailed three-dimensional models of the terrain and infrastructure. These digital models enable automated environmental analyses and support emergency services in operational and tactical planning. At the same time, they serve as the basis for digital twins of operational environments.

In addition to airborne systems, Horus3D has also been extended for robot-assisted inspection systems that can be deployed in complex indoor spaces or hazardous environments. By creating digital twins, robotic platforms can be controlled remotely while simultaneously performing automated 3D analyses of the environment. These assist specialists in analysing suspicious objects, detecting CBRNe substances and monitoring critical infrastructures.

MuFASA Software Framework

Another key technology is the Multimodal Fusion Architecture for Sensor Applications (MuFASA). This software framework enables the intelligent fusion of data from different sensor sources at the feature level. By combining spatially and temporally correlated sensor data, false alarms can be reduced and the reliability of alarm notifications can thus be significantly increased. At the same time, the modular structure allows for expansion to new sensor types and fields of application.

The combination of these technologies creates a powerful digital infrastructure for modern CBRNe situational awareness systems. The integration of sensor technology, automated data analysis and 3D environmental models produces a comprehensive situational picture that helps emergency services identify threats at an early stage and make informed decisions.

Against this backdrop, AIT has an excellent reputation as an internationally recognised competence center in the field of crisis and disaster management. The current focus is on the CBRNe components Detection Identification Monitoring (DIM) and Knowledge Management (KM). There are plans to address Hazard Management (HM) and Physical Protection (PP) in future European projects, thereby expanding the "System of Systems".

RaptoR Software Module

The RaptoR software module has been developed for radiological reconnaissance, enabling the precise mapping of radioactive contamination using unmanned aerial vehicles. During flight, sensors collect radiological measurement data, which is used to locate multiple radioactive sources and to generate dose rate maps.

In combination with the 3D analysis, even areas that are difficult to access can be precisely mapped. Furthermore, the technology enables the detection of chemical substances and the analysis of terrain structures to support automated sampling.



6 SUSTAINABLE & RESILIENT SOCIETY

The sustainable and resilient development of cities, regions and infrastructure requires data-driven decision-making and close collaboration between public bodies, infrastructure operators, businesses and citizens. Meanwhile, environmental, climate and sustainability issues are becoming increasingly complex, requiring integrated solutions that combine information from various sources and incorporate it into operational processes.

AIT develops digital solutions to support sustainability management, climate resilience, environmental monitoring, and the digital transformation of administrative and infrastructure processes. By combining data, knowledge and decision support, AIT experts lay the foundations for transparent, efficient and trustworthy collaboration within complex ecosystems. Applications range from climate change adaptation and air and water quality monitoring to sustainable agriculture and forestry, renewable energies, the circular economy and evidence-based environmental policy.

A robust understanding of the current situation is a prerequisite for effective action. At all levels, from the national to the regional, city and specific operational environments, environmental and climate data must be continuously collected, integrated and interpreted to highlight risks, pressures and development trends. This applies to the monitoring of pollutants in air and water, the assessment of climate adaptation measures and the modelling of future developments under different conditions, for example. AIT creates a sound foundation for sustainable and resilient action by combining sensor data, environmental modelling, trustworthy AI and decision-oriented analysis.

Sustainable &
Resilient Society



Digital Solutions for Protecting the Environment

In the field of Environmental Analytics, key challenges in the areas of climate, the environment and sustainability are addressed. To this end, the AIT Center develops data-driven analytical methods that contribute to the implementation of the European Green Deal's objectives. The focus is on data fusion, physically informed machine learning and explainable and trustworthy forecasting models. The fields of application range from the adaptation to climate change and sustainable agriculture and forestry to renewable energies and the circular economy.



Whether on a global scale or in specific contexts, when it comes to the environment and climate, it is first and foremost necessary to understand the current situation in order to evaluate various options for action based on this understanding. This applies to the ongoing monitoring of pollutants in the air or water, as well as the assessment and monitoring of measures and the modelling of future developments.

The solutions developed at AIT support countries, decision-makers and organisations in analysing the current situation and planning future investments. Building on the AIRDB platform for operating large sensor networks, developed by AIT in collaboration with the company ADES, solutions are offered for monitoring a wide range of environmental parameters. In addition, the EMIKAT platform was developed at AIT to identify emission sources as a basis for creating scenario models. Thus it is possible e.g. to model and objectively assess regulatory measures for the adaptation to climate change.



EMIKAT – Comprehensive Solution for the Management and Analysis of Emission Data



EMIKAT is a high-quality data management and data analysis system that provides detailed emissions and energy inventories and enables informed decision-making to reduce the release of air pollutants. The system can be used to calculate and visualise the environmental impacts of current and future “what if” scenarios. This allows e.g. the simulation of key future issues for urban planning, such as the effects of global warming or decarbonisation measures.

It provides a spatially and temporally resolved picture of end-user energy consumption as well as air pollutant and greenhouse gas emissions. The system thus enables the analysis of energy consumption and pollutant emissions for various spatial units and different time periods.

AIRDB – Intelligent Solution for Air Quality Measurement

AIRDB



AIRDB is a performant and highly precise sensor network solution for managing and monitoring large sensor networks, e.g. in the fields of air or water. As a robust yet flexible system, AIRDB is the only solution that bridges the gap between a stationary, certified “fit for purpose” solution and a modern toolbox that is also open to other industries, other measurement hardware and the integration of spatial data.

As a flexible, modern platform for experts and organisations in the environmental sector, the system's modern architecture meets all current regulatory and compliance requirements from both the technical and the IT perspective. Measurement data can be recorded independently of the measurement station computers or data loggers used and fed into an audit-proof processing workflow.

Expert functions are available via modern browser applications and can be delivered in a personalised manner based on roles and rights. Database access, topology and device management, as well as function calls for complex data aggregation (TimeSeriesEngine with FORMULA®Expressions), are available for secure integration into third-party systems via API.



Smart Cities & Municipalities

Today, cities and municipalities need concrete digital tools to make wellinformed decisions in the areas of adaptation to climate change, sustainable urban development, infrastructure planning and crisis prevention. The AIT Center for Digital Safety & Security develops practical solutions for this purpose that integrate data from various sources, present complex information in an understandable way and derive directly usable decision-making bases from that data. The systems developed are already being used in European projects and pilot regions and support cities in connecting fragmented data landscapes and planning strategic measures in a transparent manner.

Data exchange

A key solution is the development and implementation of municipal data spaces which enable secure and sovereign data exchange between public authorities, infrastructure operators, businesses and research institutions. The architectures developed by the Center integrate data from areas such as environmental monitoring, energy, mobility, buildings and climate risks into a shared digital infrastructure.

These platforms enable cities to consolidate previously separate data sources and make them usable for planning and

decision-making processes. Corresponding data space concepts have already been implemented in several European projects, for example for urban data spaces or cross-sector industrial applications. The governance models developed ensure that data sovereignty, access control and interoperability are guaranteed whilst enabling the long-term use of the systems.

Knowledge Management

To support complex decision-making processes, the Center's experts are developing AI-supported knowledge platforms that automatically index and link large volumes of documents, guidelines, scientific findings and operational data. The systems are based on semantic models and knowledge graphs and enable structured navigation through extensive information repositories.

These technologies are already being used in research projects such as NEB Junction, MAIA and AI4Health to bring together information from various research and practical projects, which is then



made accessible to users. One concrete outcome is the NEB Knowledge Hub, which links knowledge from various New European Bauhaus initiatives in a structured way, making it reusable.

This enables local decision-makers to find relevant information more quickly, to better understand interrelationships and to align their measures with existing best practices.

New European
Bauhaus



Marketplace

Together with partners, the AIT Center is developing digital platforms that serve as a marketplace for data, models and analysis tools. These platforms integrate scenario analysis, planning tools and data sources into one shared digital environment, enabling cities to systematically evaluate different options for development.

One example for this are solutions that integrate digital planning tools, sustainability indicators and infrastructure information into

existing municipal systems. This enables cities to incorporate new data sources directly into their planning processes and to compare measures for climate adaptation or sustainable urban development on a data-driven basis. The platforms are modular in design and allow new applications or data sources to be integrated step by step.



Reporting & Digital Twin

To ensure the transparent evaluation of sustainability measures, the Center develops solutions for digital monitoring, reporting and digital twins of infrastructure and buildings. Digital building logbooks and product passports enable the structured documentation of material properties, emissions and life-cycle data.

This information is linked to planning data and sustainability indicators, forming the basis for consistent sustainability reporting as well as for strategic transformation pathways towards

climate-neutral cities. In addition, digital twins make it possible to simulate different development options, e.g. for energy or infrastructure measures. This enables cities to analyse the impacts of planned measures and make informed decisions for long-term sustainable and resilient urban development.

7 ENABLING DIGITAL TECHNOLOGIES

The term “Enabling Digital Technologies” encompasses those key strategic technologies that serve as the technological foundation for future secure, resilient and sovereign digital infrastructures. They create the conditions for innovation in industry, public administration and critical infrastructure. At the same time, these technologies strengthen Europe’s technological capacity to act and its digital sovereignty with regard to the entire society.

The focus is on three core areas. New photonic sensors enable high-precision measurement and detection systems for applications in security, environmental monitoring and industry. Quantum encryption and quantum communication: these ensure long-term trustworthy and eavesdropping-proof information transmission, even in the age of powerful quantum computers. State-of-the-art wireless technologies such as 5G and 6G form the backbone of networked, latency-critical and mission-critical applications. They create the infrastructural basis for data-intensive real-time systems. Working in tandem, these technologies form the foundation for robust, high-performance and future-proof digital systems, as well as for new, scalable applications.

Optical Quantum
Technologies



Next-Generation Chip Technologies

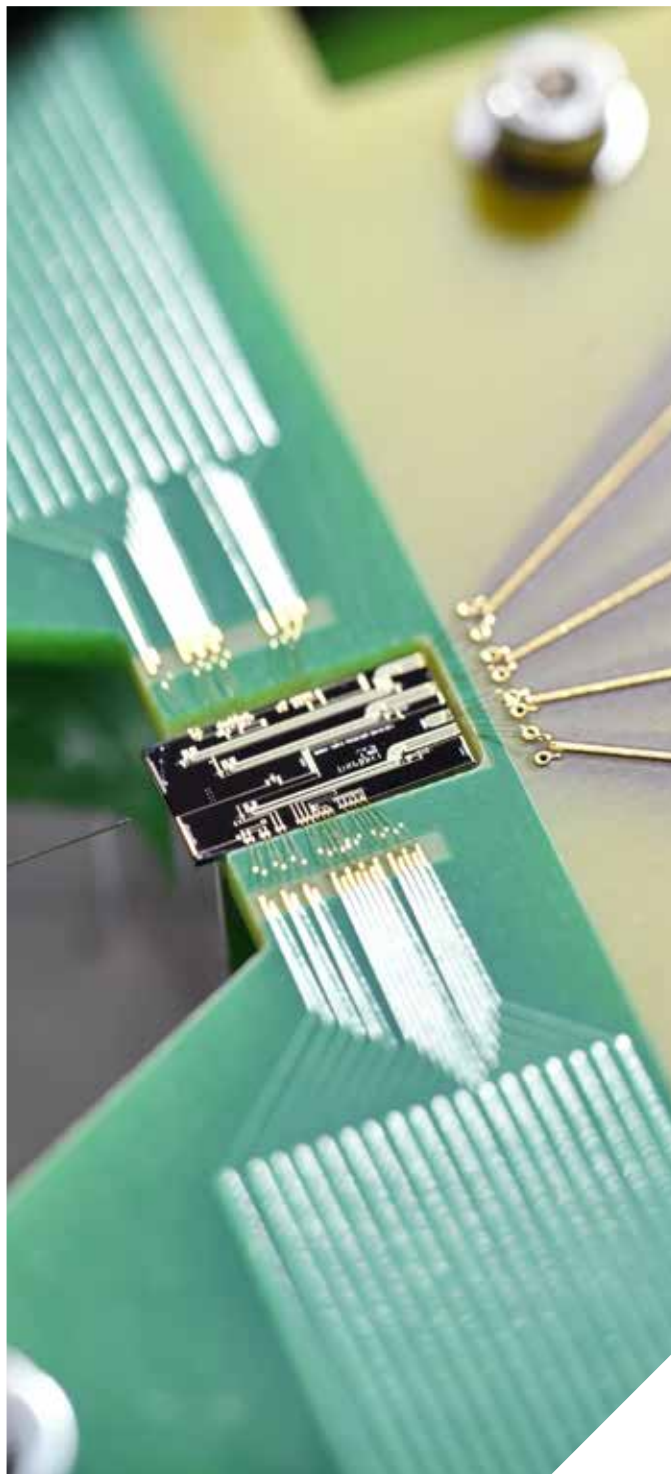
Traditional electronic components are increasingly reaching their physical and technical limits, particularly in terms of speed, energy efficiency and miniaturisation. Not least due to the rising demand for more powerful, energy-efficient and compact technologies, there is a growing need for innovative solutions such as photonics-on-the-chip. This technology enables the next generation of high-performance processors and communication systems, which are crucial for applications in the fields of telecommunications, sensor technology and quantum cryptography. The integration of photonics onto semiconductor chips – so-called Photonic Integrated Circuits (PICs) – offers a promising solution to overcome these challenges while simultaneously boosting performance. For Austria as an emerging semiconductor hub within the framework of the EU Chips Act, it is crucial to invest in this forward-looking technology sector and to build up expertise for the country.

The AIT Center for Digital Safety & Security is driving forward the development of Photonic Integrated Circuits (PICs) through leading-edge research and innovative projects on an international scale.

A case in point: AIT is actively involved in prestigious photonics technology programmes and acts as project coordinator for the European Innovation Council (EIC) Pathfinder project QOSiLICI0US. Furthermore, it has been granted the “Photonics 4 Quantum” (P4Q) Framework Partnership Agreement under the Chips JU Quantum Chip Technology Programme to establish production capacities for the manufacture of photonic chips and components for applications in quantum technology. With this expertise and by establishing the AT-C3 Chip Competence Center, AIT has also positioned itself within the EU Chips Act initiative and is making this specialised know-how available to the Austrian manufacturing industry.

The Center's experts are currently working on realising a silicon-based light source. This monolithic approach to quantum-optical integrated circuits is fully compatible with the electronics industry's wafer fabs and also allows for the seamless co-integration of optical quantum technologies into electronic processors. This holds out the prospect of extremely cost-effective manufacturing of chip-based quantum-optical systems in the future, such as those required for information-theoretically secure quantum cryptography.

With these excellent developments, AIT is making a decisive contribution to strengthening Austria's position as a semiconductor hub within the framework of the EU Chips Act.



QOSiLICI0US



AT-C3



Photonik



Quantum Encryption

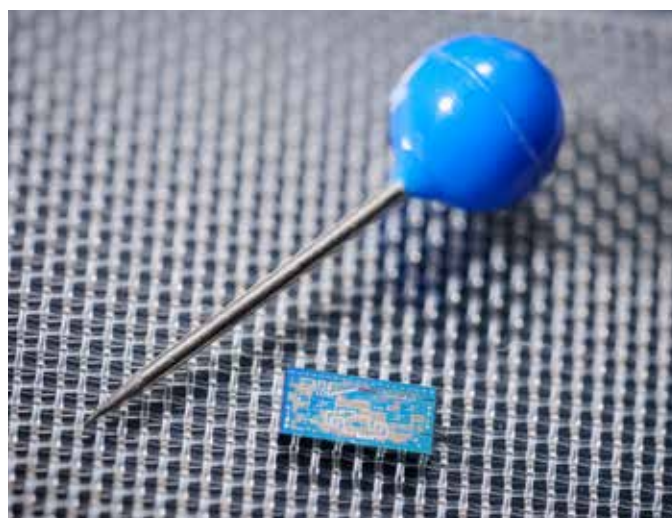
Building on the fundamental research of the distinguished Austrian Nobel laureate Anton Zeilinger, AIT, through its Center for Digital Safety & Security has very successfully positioned itself in the field of quantum technologies as an essential source of expertise and technology supplier for the EU's technology implementation strategy, as well as for the establishment of a European manufacturing industry for quantum encryption (Quantum Key Distribution – QKD). Today, as a leading international competence center for both terrestrial and satellite-based quantum cryptography – for example, within the framework of the EU programmes EuroQCI (fibre-optic infrastructure) and IRIS2 (satellite infrastructure through the SAGA and EAGLE programmes) – AIT is spearheading key implementation initiatives for a secure, connected Europe.



The establishment of a quantum-secure network in Austria has already been successfully demonstrated, comprising an inner-city computer network linking four federal ministries and a long-distance link from Graz to Vienna. To replicate real-world conditions, a wide range of applications have been developed, including secret sharing, video chat and data backups. These were secured using QKD. The expertise of the AIT Center for Digital Safety & Security also forms an important basis for dedicated strategic advisory activities in the sense of the European Commission regarding the development of an EU standardisation strategy and an EU QKD technology strategy. AIT holds approximately 30 patents in this high-tech field.



These activities are carried out as part of substantial technology development contracts awarded by ESA, industry organisations and the European Commission to establish specialised testing and verification capabilities within the EU (Nostradamus project). These include major technology pilot projects in all Member States, such as the Digital Europe Programme (DEP) with projects like QCI-CAT and. A further focus is on projects aimed at establishing technology providers (supply industry) within the EU Quantum Flagship Programme as well as the Digital Europe Programme, such as eCausis and Quarter. This also includes the development of a manufacturing industry in the EU through EU projects such as Q-Test and Q-Pilot.



EuroQCI



IRIS2



QCI-CAT



PETRUS

Open QKD
TechnologyQuantum
Technology

Next-Generation Wireless Technologies

With advancing digitalisation and the emergence of autonomous systems, there is a growing need for reliable, secure and energy-efficient wireless communication solutions for safety-critical applications in industry as well as in road, rail and air transport. Safety-critical applications such as autonomous vehicles, Industry 4.0 or public transport systems require wireless communication solutions that guarantee the highest levels of reliability and security. Conventional wireless technologies are reaching their limits here, particularly when it comes to latency and reliability. There is an urgent need for innovative technologies that meet these requirements and simultaneously serve as test platforms for future communication standards such as 6G.



The AIT Center for Digital Safety & Security possesses leading scientific and technological expertise in Austria in the field of the next-generation 6G wireless technology and is now successfully established within the EU industrial ecosystem with innovative, reliable, wireless and energy-efficient developments in the field of communication technologies. The Center has successfully implemented the world's first 6G technology components with Software Defined Radio (SDR) components as a proof of concept.

6G technology components include widely distributed antenna systems, reconfigurable and intelligent surfaces as well as multi-band radio systems. For these three technology areas, control and signal processing methods for integrated communication and localisation have been developed. As basis technology, the Center has researched novel radio channel measurement techniques and numerical simulation methods building on geometry-based models for 6G systems. At the same time, test methods for radio systems based on machine learning have been established. Furthermore, through the Center, AIT is leading the international standardisation activity within the framework of IEEE P1944 for geometry-based radio channel models, which are a central component of the research and test methods for 6G communication and localisation systems.

Key use cases include autonomous rail transport, autonomous freight wagons, safer operation of unmanned aerial vehicles (UAVs), improved road safety through sensor data exchange between road vehicles, and much more. Furthermore, in future, radio systems will offer localisation capabilities in addition to data communication. Against this backdrop, AIT has successfully established R&D partnerships with leading Austrian and EU industries such as Siemens, ÖBB, AVL and Ericsson, as well as Thales. Moreover, AIT holds significant patents in this high-tech sector.



8 INITIATIVES AND PLATFORMS

Trustworthy digitalisation, digital sovereignty and societal resilience do not emerge in isolation, but through strong networks, shared platforms and international cooperation. Technological innovation must be aligned with regulatory requirements, social responsibility and practical feasibility. Strategic initiatives and cooperation platforms therefore play a central role in bringing together stakeholders from research, industry, public administration and international politics to exchange knowledge and expertise.

Initiatives such as the Gaia-X Hub Austria, the International Digital Security Forum (IDSF) and the PeaceTech Alliance create concrete spaces for exchange, community-building and the development of trustworthy digital ecosystems. They make an active contribution to sustainably strengthening European values, technological innovation and international cooperation in the digital sphere and translating them into practical implementation.

Gaia-X Hub Austria

Data has become a strategic resource for business, administration and society. At the same time, there is a growing awareness that its use requires clear rules, trust and technological sovereignty. This is because organisations are increasingly faced with the challenge of sharing data across corporate, sectoral and national boundaries without losing control, compliance or competitiveness. In addition, trust, clear roles and technical enforceability are not merely theoretical requirements but operational necessities, particularly in critical sectors such as energy, industry, security and public administration. Data spaces must therefore not only be conceptually sound but also scale in real-world operations, meet regulatory requirements and deliver measurable added value.

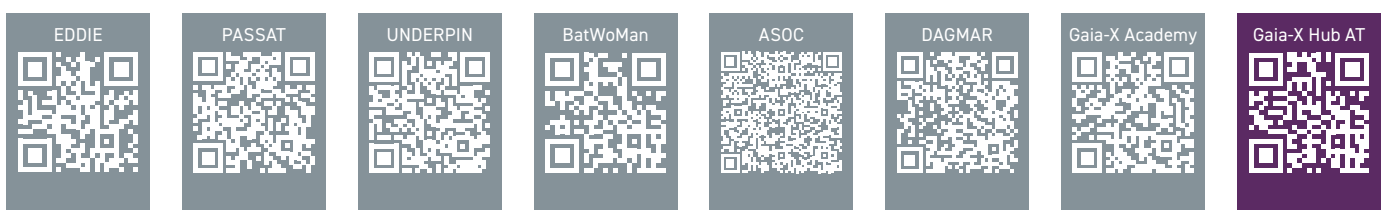
The Gaia-X Hub Austria plays a key role here as a central pioneer for trustworthy, interoperable data spaces, thereby enabling European values like transparency, security and self-determination to be put into practice. In order to support data sovereignty objectives in the EU and to promote the development of a new, data-driven ecosystem, AIT, with its Center for Digital Safety & Security, has successfully and significantly established the Gaia-X Hub Austria on behalf of the Federal Ministry for Innovation, Mobility and Infrastructure (BMIMI) and the State Secretariat for Digitalisation in the Federal Chancellery (BKA). This serves to accelerate European data ecosystems for economic, environmental and societal value creation. The Gaia-X Hub Austria has thus proven itself as a bridge-builder between the European framework and national implementation. Through targeted networking of industry, research, administration and politics, the Hub supports the concrete application of Gaia-X principles in real-world projects.

Moreover, the AIT Center has also established itself as a steering board member within the EU Gaia-X initiative. Initiatives such as EDDIE (Energy Data Room), PASSAT (Digital Product Passport) and UNDERPIN (Manufacturing) clearly demonstrate that data rooms in Austria are no longer pilot projects, but can deliver practical added value across various sectors. Another milestone is the DPP demonstrator from the BatWoMan project, which serves as a blueprint for the implementation of a battery passport. The demonstrator concretely shows how normative requirements from current and upcoming EU regulations, particularly in the context of the Digital Product Passport, can be technically implemented and integrated into existing value chains.

In the security sector, too, KIRAS projects such as ASOC und DAGMAR underscore that sovereign data rooms are a key element in tackling hybrid threats and protecting critical infrastructures. In the context of the PeaceTech Alliance, together with the Austrian Center for Peace (ACP) and further partners, it also becomes clear how data spaces can support trust, cooperation and resilience, even in international and security-policy-sensitive environments.

The Hub thus positions itself not only as a coordination point, but as an active accelerator for the implementation of digital sovereignty in Austria, with a clear focus on real-world use cases and regulatory feasibility.

With the Gaia-X Academy, the Hub also provides a freely accessible, online-based training programme that introduces companies, organisations and individuals to the concepts, technologies and governance models of data spaces in a practical manner. This builds targeted know-how to facilitate entry into Gaia-X-compliant data ecosystems and to increase the programme's broader impact. These developments underline Gaia-X Hub Austria's commitment not only to providing strategic guidance but also to offering concrete support to companies in implementing regulatory requirements and establishing future-proof, sovereign data spaces.



International Digital Security Forum (IDSF)

Security is a key prerequisite for the deployment of digital technologies. Recent developments such as artificial intelligence (AI), the Internet of Things (IoT), biometric methods for digital identity management, cloud-based services and global networks open up innovative application possibilities, but at the same time have disruptive effects on existing systems, markets and social structures. Cyber security, in particular, places high demands on system developers, service providers and users.

As digital technologies become increasingly democratized, new threat scenarios are emerging whose scope and scalability are increasingly pushing traditional protective mechanisms at both organisational and government levels to their limits. The evolving threat landscape therefore requires a new understanding of critical infrastructures, as well as innovative approaches to strengthening their resilience.

At the same time, international coordination, confidence-building measures and a structured information exchange are becoming increasingly important in order to respond appropriately to global risks. However, all of this must be done in accordance with universal human rights, which primarily guarantee both the freedom of expression and the right to privacy.

Against this backdrop, the International Digital Security Forum (IDSF) was launched in 2020 as a new format for international exchange and community building; its fourth edition was held in Vienna in June 2025. The IDSF is organised by the AIT Austrian Institute of Technology with the support of the Federal Ministry for European and International Affairs (BMEIA) and other key Austrian federal ministries. It is run in close collaboration with the Austrian Security & Defence Industry Group (ASW) of the Austrian Federal Economic Chamber (WKO), the Competence Center Secure Austria (KSÖ) and the Agency for Economic Cooperation and Development (AED), in cooperation with international partner organisations.

INTERNATIONAL DIGITAL SECURITY FORUM VIENNA

The IDSF is based on three central pillars:

- 1) It addresses the security and socio-political challenges arising from the use of new digital technologies.
- 2) It specifically brings together all relevant stakeholders in the digital security landscape, ranging from government decision-makers at national, European and international levels to representatives from industry, research, academia, the media and civil society.
- 3) The forum relies on innovative formats and tools for knowledge exchange, discussion and awareness-raising, combining in-person formats with digital presentation options.

These three pillars form the basis for the ambition to establish the IDSF as a uniquely international space for dialogue. Beyond individual events, the Forum contributes to the development of a widely recognised platform for international discussion and cooperation. The aim is to promote common frameworks, rules and a shared understanding so that digital technologies serve people and society in the long term.

Vienna as the venue underscores this ambition. Austria's international role and its tradition as a neutral mediator create ideal conditions for open, cross-border and trust-based discussions in the global context of digital security.



PeaceTech Alliance

The PeaceTech Alliance is an international, non-profit platform dedicated to the responsible use of digital technologies for peacebuilding, conflict prevention and societal resilience. It is founded on the conviction that technology has considerable potential to support peace processes, for example through improved information bases, the use of artificial intelligence (AI), new forms of cooperation or capacity-building for local actors. At the same time, it emphasises that this potential can only be realised if technological innovations are accessible, context-sensitive and designed in a value-based manner.

The PeaceTech Alliance was launched in 2025 by the AIT Austrian Institute of Technology in collaboration with the Gaia-X Hub Austria as part of the 4th International Digital Security Forum (IDSF) in Vienna. It builds on a strong interdisciplinary partner network that reflects Austria's unique role at the intersection of peacebuilding, diplomacy, science and technology. Initial partners include the Austrian Center for Peace, the International Institute for Peace, the Open Knowledge Foundation, the Diplomatic Academy of Vienna, and academic institutions such as the University of Innsbruck, the University of Graz and the University for Continuing Education Krems. International perspectives are contributed by the Open Knowledge Foundation, amongst others.

Exchange, expertise and collaboration are at the heart of all activities. The PeaceTech Alliance offers events, workshops and training formats, as well as practical content via blogs, podcasts and toolkits that present technological approaches in an accessible



PeaceTech Alliance

*Austria's Global Hub for
Peace Technology*

way and highlight concrete use cases. In addition, digital projects and open-source tools are being developed to support peace actors in making their work safer, more effective and more sustainable. A particular focus is on involving civil society as a co-creator of technological solutions, rather than merely in its role as a user.

Another key focus of the initiative is the development of federated, trusted data spaces for peace and security-related use cases. Building on the principles of Gaia-X, the PeaceTech Alliance aims to enable sovereign data exchange and promote collaboration without compromising control, accountability or data protection. Such structures lay the foundation for trust between stakeholders in government, the civil society and on an international level in an increasingly data-driven world.

Rooted in Austria's self-image of neutrality and dialogue, and supported by a growing network of national and international partners, the PeaceTech Alliance positions itself as an open space for cooperation on responsible digital innovation. In doing so, it contributes to the further development of a humane, inclusive and future-oriented understanding of technology, with the clear aim of consistently putting digital tools at the service of peace, trust and social stability.

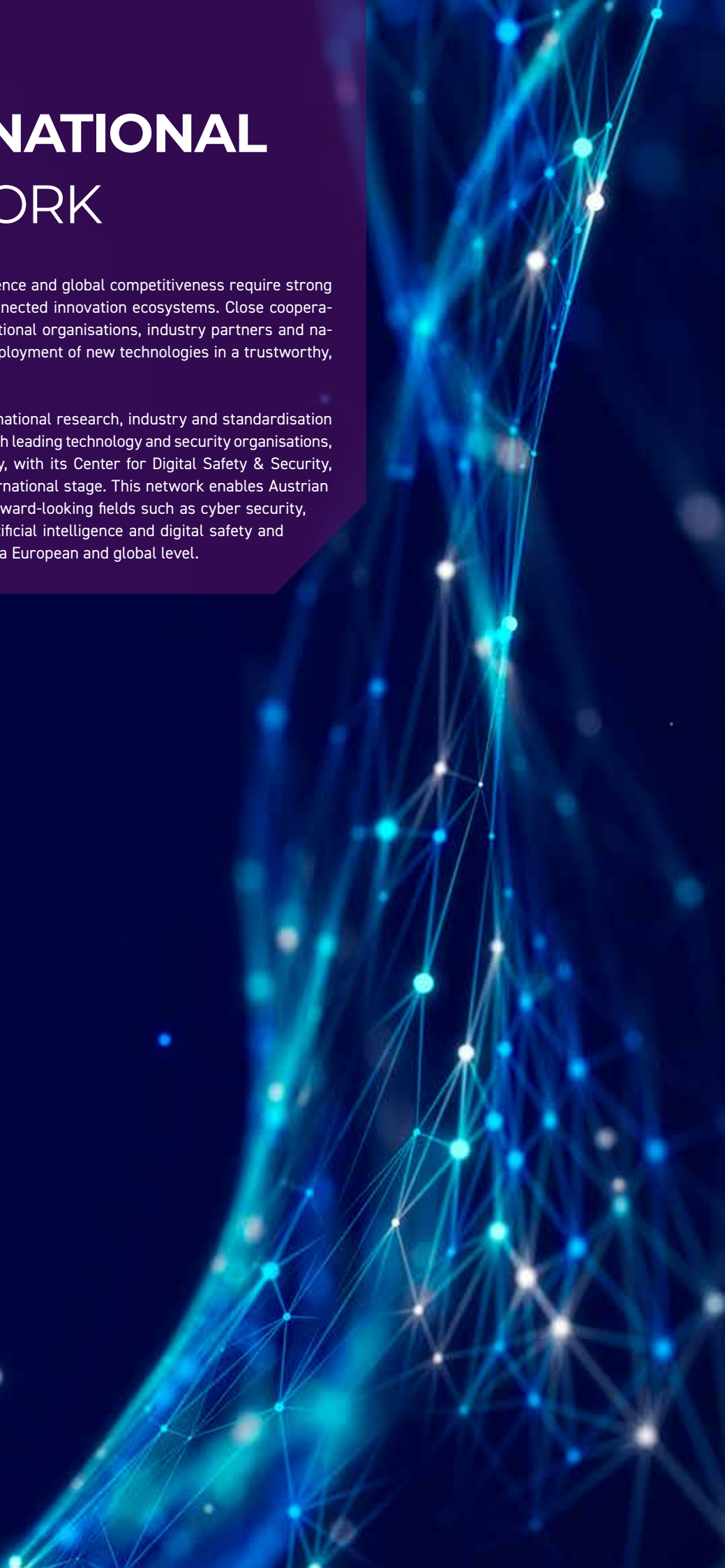
PeaceTech
Alliance



9 INTERNATIONAL NETWORK

Digital sovereignty, technological resilience and global competitiveness require strong international partnerships and interconnected innovation ecosystems. Close cooperation with European institutions, international organisations, industry partners and national authorities is essential for the deployment of new technologies in a trustworthy, interoperable and scalable manner.

Through its active involvement in international research, industry and standardisation initiatives, as well as its collaboration with leading technology and security organisations, the AIT Austrian Institute of Technology, with its Center for Digital Safety & Security, has firmly established itself on the international stage. This network enables Austrian technological expertise in strategic, forward-looking fields such as cyber security, quantum technologies, data spaces, artificial intelligence and digital safety and security to be sustainably positioned at a European and global level.



International Network

In general, the AIT Center for Digital Safety & Security holds a recognised position in national and international innovation programs such as KIRAS and Horizon Europe and is a constitutive part of industry and research initiatives such as the Quantum Communication Infrastructure Europe (QCI), European Cyber Security Organisation (ECSO), Public Safety Communication Europe (PSCE), Electronic & Software Based Systems (ESBS) or the Task Force of European research organisations in the security context (EARTO/EUROTECH). In this respect, the Center cooperates with international organisations such as the International Atomic Energy Agency (IAEA), the Organisation for Security and Cooperation in Europe (OSCE), the United Nations Office on Drugs and Crime (UNODC), the United Nations Office of Counter-Terrorism (UNOCT), and the Vienna Center for Disarmament and Non-Proliferation (VCDNP). At the national level, the Federal Ministry of the Interior (BMI) and the Federal Ministry of Defence (BMLV) are key partners. This has laid a solid foundation for establishing Austrian technological innovations and the associated expertise on the international stage, as the following summary shows.

With its Center for Digital Safety & Security, the AIT Austrian Institute of Technology is one of the key players in the European EuroQCI and IRIS2 communities and is also regarded by the European Commission (EC) as a key stakeholder in the implementation of the EC's objectives in the field of quantum communication. This is demonstrated by its broad integration across all areas of EU programmes, through industrial collaborations with leading EU industries such as Deutsche Telekom, Thales and Airbus, as well as through its explicit involvement as a strategic advisor to the EC. Furthermore, the Center has successfully established itself in this field within the EU space/satellite industry as a technology supplier to the ESA and to leading EU industry partners such as Deutsche Telekom (D), Thales (F), OHB (D), SES (Lux) and Thales Alenia Space (I).

This strong expertise in the field of quantum technologies, combined with the competence in photonics technologies, 6G wireless technology, as well as a secure embedded system development and cyber security, also forms the basis for positioning AIT within the Austrian Electronic & Software Based Systems (ESBS) community. AIT – together with key semiconductor industry players like Infineon, AMS/Osram, AT&S and AVL – thus helps promote Austria as a high-tech location.

In order to implement the EU's data sovereignty objectives, AIT with its Center for Digital Safety & Security has successfully established itself within the EU network for the development of federated

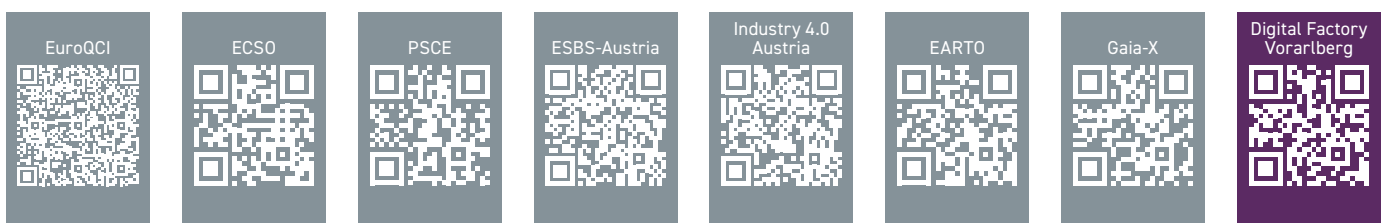
data systems. Through the activities of the Center, Austria is a recognised stakeholder within the network of the international Gaia-X hubs and has also positioned itself as a key national player in the data platform scene in Austria. This development is evidenced by the successful cooperation with the Federal Ministry for Innovation, Mobility and Infrastructure (BMIMI) and the State Secretariat for Digitalisation. Furthermore, this Austrian research institution is also represented on the board of the EU Gaia-X Initiative.

To support the digital transformation, particularly in the areas of cyber security, artificial intelligence and sensor systems (IoT), AIT cooperates with Austria's national industry, plays an active role in the key network communities within the Industry 4.0 Austria platform.

In the field of cyber security, AIT has established a successful position within the network of international security organisations. AIT, and thus Austria, is currently the only IAEA "Collaborating Center" for IT security. Moreover, the AIT Center also regularly conducts international training courses in collaboration with the World Institute for Nuclear Security (WINS) and the United Nations Office for Counter-Terrorism (UNOCT). Building on this, AIT also acts as a key network partner for the Austrian Federal Ministry for European and International Affairs (BMEIA). At the national level, AIT has established itself as a recognised expert in cyber security through its Center for Digital Safety & Security. This is reflected in its active involvement in key national network organisations such as the Competence Center Secure Austria (KSÖ), the Cyber Security Platform (CSP) of the Federal Chancellery, Digital City Vienna, the Vienna Cybersecurity and Privacy Research Cluster (ViSP), and finally through its established role as an implementation partner in the ongoing national cyber security simulation exercises organised by the Federal Ministry of the Interior (BMI) in collaboration with the national network of critical infrastructure operators.

Digital Factory Vorarlberg – A Knowledge Center for Digitalisation

An interdisciplinary project team comprising FH Vorarlberg and the AIT Center for Digital Safety & Security, coordinated by Wirtschafts-Standort Vorarlberg GmbH (WISTO), has established Digital Factory Vorarlberg, a dedicated research Center for the Vorarlberg region. Linking the regional university with the expertise of Austria's largest non-university research center opens up access to international research networks, creates cross-organisational research capacity and expertise, and makes these available to companies in Vorarlberg.



10 SELECTED RESEARCH INFRASTRUCTURES

The Center has a strong focus on software-based development and research activities. Specialised research infrastructures have been established for three selected high-tech sectors, serving as the foundation for internationally competitive cutting-edge research whilst enabling a high number of collaborations with academic and industrial partners.





Photonics & Quantum Communication Laboratory

The Photonics & Quantum Communication Laboratory addresses technologies based on the use of light. The activities of the research groups in this field range from photonically integrated circuits at the chip level, via system integration of optical and electronic components, all the way to demonstrating new applications in telecommunications, quantum optics and sensor technology.



The research laboratory is equipped with a test station for controlling and measuring photonic chips, with a wide range of instruments for optical and high-frequency signal generation and analysis from nanometres to terahertz, as well as with superconducting nanowire detectors for measuring single photons.

Thanks to the lab infrastructure established at the Center for Digital Safety & Security, AIT is able not only to design quantum communication components and systems and measure them, but also to make the lab available in Europe as a test facility. The quantum optical components and systems comprise various types of QKD implementations, such as transmitters and receivers for CV, DV, entanglement-based and measurement-device-independent QKD systems, "on the chip" or as optical systems, quantum random number generators, neuromorphic optical chips and similar subsystems.

Radio Frequency Laboratory

Secure and reliable electronic communication links are a key prerequisite for a modern society. The Wireless Communication and Sensing research group is working on new methods to exploit the physical properties of wireless communication media in order to ensure security and protection and to determine the position of objects.

In the area of wireless communication, novel communication and localisation methods for 5G/6G systems are being developed so as to enable ultra-reliable, low-latency communication links with precise positioning. They can make sure that e.g. cables can be replaced by wireless systems in production environments, or that autonomous vehicles and trains can operate reliably.

This laboratory infrastructure makes it possible to address a wide range of research and application questions relating to communication and localisation systems.

A case in point: radio channel emulations can be offered for "hardware-in-the-loop" testing. This also includes millimetre-wave radio systems capable of determining the positions of objects indoors with centimetre-level accuracy by way of using novel reconfigurable and intelligent surfaces.



AIT Cyber Range – Test & Training Center

Building on AIT's technological and research expertise and its mission to support Austrian society, critical infrastructure providers and businesses, cyber security training sessions and exercises are held on a regular basis. To this end, a unique digital and hybrid simulation platform, the AIT Cyber Range, has been developed. Since 2017, national simulation exercises have been conducted in cooperation with the Competence Center Secure Austria (KSÖ), involving the public sector as well as stakeholders from business and industry.

Since then, the AIT Cyber Range and its team have developed into a world-class facility. In line with this development, AIT currently functions as the world's only IAEA Collaboration Centre on the topic of cyber security for nuclear safety, supporting global training activities through the Center.

This education and training infrastructure complements research activities, enabling the evaluation of new defence technologies as well as new threat scenarios together with infrastructure operators, manufacturers and security officers, with the aim of building concrete practical capabilities.



11

CERTIFICATIONS

In order to conduct research and development in line with the increasing security requirements of public authorities and industrial clients in the field of digitalisation while meeting the highest standards of information security, the AIT Center has established specialised processes and expertise and built up a corresponding security infrastructure. It is thus approved to work on classified projects at the "EU Restricted" security level. In this context, AIT has also obtained the necessary certification from the Austrian authorities.

Thanks to its comprehensive expertise in handling classified information, official certification by the Federal Ministry of Defence (BMLV), and the associated special security measures within the organization – which also include security vetting of staff – the AIT Center for Digital Safety & Security is able to carry out confidential and security-relevant research projects in compliance with the law and with the highest integrity. These prerequisites form a central basis for close cooperation with both national and international authorities, as well as industry partners who place the highest demands on the protection of sensitive data and information.

 Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria

 Federal Ministry
Finance
Republic of Austria



 Federal Chancellery
Republic of Austria

 Federal Ministry
Interior
Republic of Austria

 Federal Ministry
Defence
Republic of Austria

Through close collaboration with public authorities and Austrian companies, the AIT Center for Digital Safety & Security has been able to develop specialist expertise, capabilities and new technological solutions in a number of areas. The national security research programmes KIRAS, KPASS (for cyber security) and FORTE are an important basis for launching leading international initiatives.

The activities and developments described in this publication were also significantly shaped by strong strategic partnerships and further national and international funding programmes.

We would like to extend our special thanks to the funding bodies and the numerous partners from business, industry, academia and the public sector, whose commitment and long-term support make a significant contribution to the further development of trustworthy digital security solutions and to strengthening digital sovereignty in Austria and Europe.

IMPRINT

Publisher / Media Owner

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

Images

AIT Austrian Institute of Technology GmbH
Getty Images

Place of Publication

Vienna, June 2026

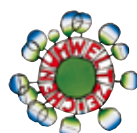
Responsible for the Content:

Editorial Team

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

Design, Layout and Typesetting

Cayenne Marketing Agency GmbH

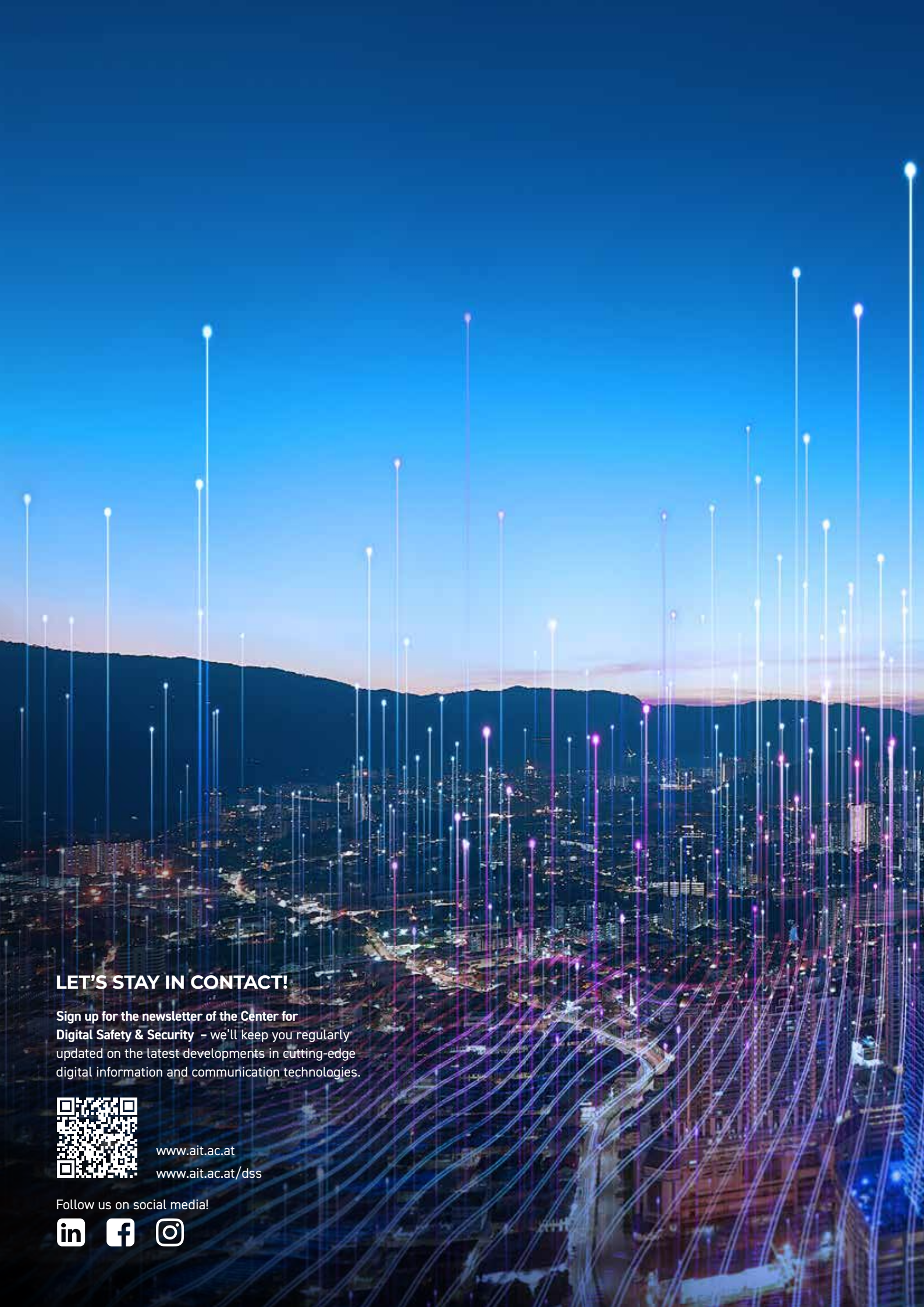


Produced in accordance with the guidelines of the Austrian Ecolabel,
Gradwohl Printproduktionen Ges.m.b.H., UW 1506

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



www.ait.ac.at

An aerial night view of a city, likely Vienna, with a river and hills in the background. The image is overlaid with numerous vertical lines of light in blue, purple, and white, each ending in a small glowing dot, creating a digital or network-like effect.

LET'S STAY IN CONTACT!

Sign up for the newsletter of the Center for Digital Safety & Security – we'll keep you regularly updated on the latest developments in cutting-edge digital information and communication technologies.



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

Follow us on social media!

