INTERNATIONAL DIGITAL SECURITY FORUM *VIENNA*

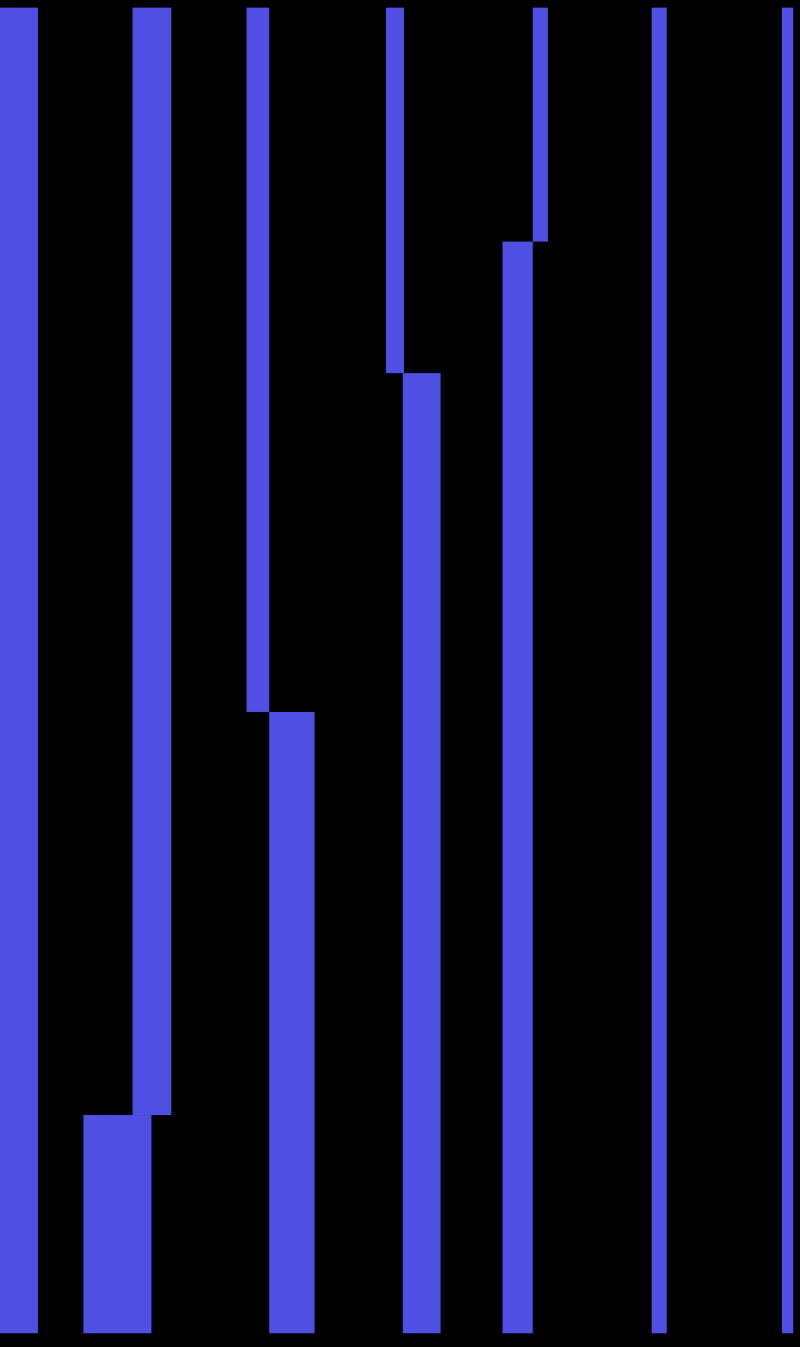
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

KSÖ Kompetenzzentrum Sicheres Österreich

WKO WIRTSCHAFTSKAMMER ÖSTERREICH
ARGE Sicherheit & Wirtschaft

PROGRAM PARTNER

VICESSE



Selected Initiatives,
Projects & Technologies

INNOVATION BRIEFING

INTERNATIONAL DIGITAL SECURITY FORUM *VIENNA*

IDSF25

Balancing Sovereignty and Solidarity in the Digital Age.

This collection brings together a curated selection of forward-looking initiatives, groundbreaking technologies, and visionary projects presented by companies and organizations shaping the future of digital innovation.

Compiled for the IDSF community, the Innovation Briefing is designed to spark dialogue, foster collaboration, and serve as a catalyst for new ideas and partnerships. Each contribution offers a concise insight into current developments and emerging solutions — a source of inspiration for meaningful exchange throughout the conference and beyond.

Content

Preparedness for Humanitarian Assistance and Peacebuilding in West Africa – Become a partner!

The Project and its Impact

The humanitarian situation in many West African countries has severely deteriorated and the need for humanitarian assistance and sustainable peacebuilding approaches is high, as is the need for coordinated approaches and well-trained staff working in this field. The project provides high-level capacity training courses for West African participants from state agencies, the security sector, and civil society, including equal participation by women and mentorship for young professionals. Over the course of 4 years, we will reach 1200 direct beneficiaries who will be trained in courses about humanitarian assistance and peacebuilding, including specializations on gender-responsive climate action. In addition, we will facilitate cross-border workshops and lasting local initiatives to bring together stakeholders from Ghana, Burkina Faso, Côte d'Ivoire and Togo to foster dialogue and improve cooperation for emergency response. The project includes digital components such as self-paced learning courses, and working with digital tools for crisis response and peacebuilding. We will apply Environmental Peacebuilding as an important approach to create long-lasting and sustainable peace, which includes social cohesion and a healthy environment in times of climate crisis.

Impact
Contribute to sustainable peace, reduced vulnerability, and enhanced conflict and crisis resilience of communities in the West African region through strengthened humanitarian-development-peace nexus approaches.

Project Duration
September 2025-August 2029 (4 years)

Primary Target Group
Professionals from civil protection authorities, security forces, and civil society, with a particular focus on women and youth

Target Countries
West African region, particularly Ghana, Burkina Faso, Togo, Côte d'Ivoire - cross border region

Mainstreaming Topic
Gender & Intersectionality

Focus Topic
Environment, Climate, Peace & Security

Stakeholders
Implementing Partners: Austrian Centre for Peace (Lead Applicant), CARE International, Kofi Annan International Peacekeeping Training Centre (KAIPTC)
Funding partners: Austrian Development Agency, Austrian Ministry of Defense

Existing Project Partners

Building on previous project phases since 2013, the project is implemented by the ACP, the KAIPTC, CARE International & CARE Ghana. They hold year-long experience in capacity building in West Africa. The project is 90% funded by the Austrian Development Agency and the Austrian Ministry of Defence. For the remaining 10%, we are looking for new partners.

Become a Partner

We are looking for private sector partners and foundations in the Austrian Institute of Technology (AIT) network who want to increase their visibility in the field of humanitarian assistance and peacebuilding, both in West Africa and Europe. Our alumni form a network of 1000+ professionals in different sectors, interested in new cooperations and opportunities. You can become a partner of the project and contribute by sponsoring individual West African talents or full activities in the West African Region. Interested? Reach out to us!

Contact

Austrian Centre for Peace
Sophia Stanger, Project Manager
Rochusplatz 1
A-7461 Stadtschlaining
Austria – Europe

stanger@ac4p.at
www.ac4p.at

Cooperation – the key to a secure and prosperous Europe

The ability of a state or organization to hold control over its digital infrastructures, data and technologies is crucial to maintain its independence and security. Cybersecurity therefore plays a central role in ensuring Europe's prosperity and democratic values. Increased attacks by malicious state actors and a disconcerting rise in cybercrime demonstrate the importance of international solidarity and cooperation to strengthen our digital resilience and sovereignty.

Increasing resilience and growth by sharing best practice

With Best Practice Austria, the Federal Government has launched an initiative to strengthen Austria's global role in administrative reforms and international collaboration. The targeted cooperation between the public and private sectors enables innovative reform projects by supporting partner countries in the implementation process and by facilitating knowledge exchange.

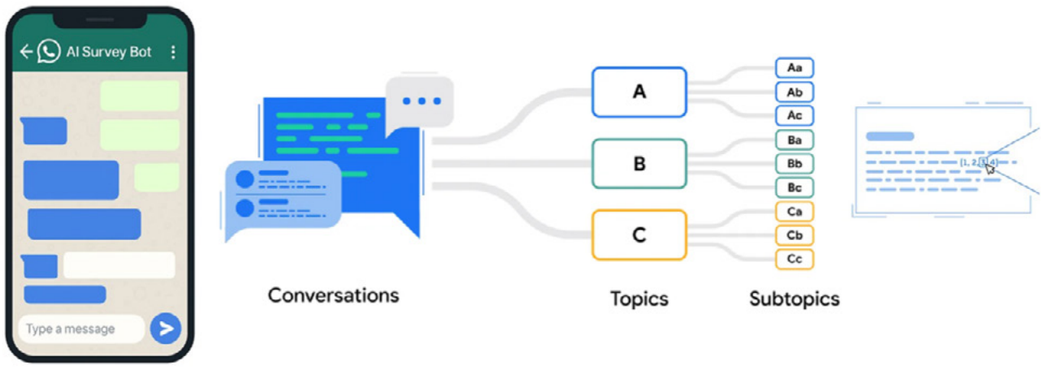
Based on individual country requests, government programmes, bilateral memoranda of understanding, EU-programmes and recommendations by international donor institutions as well as on Austrian governmental strategies for international cooperation, Best Practice Austria acts as interface between public authorities and the private sector.

The Agency for Economic Cooperation and Development (aed) is responsible for implementing the initiative. It supports intergovernmental agreements and institutional cooperation on behalf of and in cooperation with the Federal Administration and ensures the transition from project ideas to funding applications, assisting with project submissions, project execution and evaluation.

https://aed.or.at/en/homepage/
Contact: office@aed.or.at

CMI 25
MARTTI AHTISAARI
PEACE FOUNDATION

Amplifying Youth Voices in Conflict Zones: AI-Powered Digital Tools for Inclusive Dialogue in Yemen



The decade-long conflict in Yemen has fractured political participation and marginalized youth voices—a critical demographic representing 69% of the population—from peace processes. Traditional dialogue approaches face significant barriers: security risks, geographical fragmentation, and limited infrastructure. CMI presents an innovative digital engagement methodology deployed in Yemen during January-March 2025 that overcame these barriers through AI-powered crisis computing.

Our approach integrated two complementary technological solutions: a customized WhatsApp-chatbot and an AI-powered qualitative analysis tool, which extracts key insights from a large volume of input and organises them into thematic clusters, highlighting the most relevant and contested issues. The WhatsApp chatbot enabled accessible engagement across conflict lines, featuring multilingual support, interactive sequences, and voice message processing with OpenAI transcription/translation services. The methodology included 7 comprehensive survey questions alongside demographic profiling, enabling participants to submit detailed responses in Yemeni Arabic through voice messages, enhancing authenticity and depth of engagement.

Field implementation successfully engaged 142 participants across 18 governorates with a 94.53% completion rate of all survey questions, representing diverse political affiliations (eight parties/components), age groups, and genders (36.76% female participation). The T3C Sensemaking Tool ("Talk to the City") utilized computational linguistic models to analyze these highly detailed and considerate responses, identifying key topics including views on political vision, obstacles to implementation, and opportunities for youth involvement—providing actionable intelligence for mediators and policymakers supporting Yemen's peace process.

This case demonstrates how AI-powered tools can operate effectively in crisis settings by: (1) bypassing physical security barriers through digital engagement; (2) processing multilingual qualitative data at scale; (3) identifying cross-cutting themes across political divides; and (4) amplifying traditionally marginalized voices. The methodology provides a replicable framework for crisis computing applications in conflict zones where traditional engagement is restricted or impossible, with particular relevance for contexts requiring remote stakeholder consultation, sentiment analysis in fragmented societies, and inclusive dialogue processes in ongoing conflict settings.

Contact

Michele Giovanardi
Programme Officer CMI
michele.giovanardi@cmi.fi

Felix Kufus
Advisor CMI
felix.kufus@cmi.fi

OSCE Organization for Security and Co-operation in Europe

Cybersecurity in focus: advancing regional cooperation by building trust

The Organization for Security and Co-operation in Europe (OSCE) plays a pioneering role in enhancing cyber/ICT security, in particular by reducing the risks of conflict stemming for the use of Information Communication Technologies (ICTs) by its participating States.

What is cyber/ICT security?

The use of ICTs by states has had a profound impact on foreign relations, shaping how states interact, influence and engage with each other in cyberspace. This added complexity has increased the likelihood of misperception, escalation and tension.

To address this issue, OSCE participating States have developed and adopted two sets of confidence-building measures (CBMs) to reduce the risks of conflict stemming from the use of ICTs by states.

Building confidence in cyberspace

In 2012, an open-ended Informal Working Group (IWG) was established under the auspices of the Security Committee (Permanent Council Decision No. 1039). The IWG has the mandate to elaborate CBMs to enhance inter- State co-operation, transparency, predictability and stability.

The work of the IWG has led to the adoption of two sets of CBMs for cyberspace:
- Eleven transparency measures adopted in 2013, which promote cyber resilience and preparedness, encourage communication and increase transparency (Permanent council Decision No. 1106)
- Five co-operative measures adopted in 2016, which further address effective communication channels, public-private partnerships (PPPs), critical infrastructure protection and the sharing of vulnerability information (Permanent Council Decision No. 1202).

The 16 CBMs aim to build multilayered relationships based on openness and co-operation and lay a foundation for the peaceful resolution of disputes in cyberspace. Whilst the measures are non-binding, all 57 participating States have made a political commitment to adhere to them.

Supporting United Nations efforts

CBMs are an important element of the international framework of responsible state behaviour in cyberspace, which was developed at the United Nations (UN). As such, OSCE efforts in cyberspace are closely interlinked with the work of the UN in this area. As a regional organization, the OSCE acts as an implementer of UN-level agreements through practical and action-oriented work. It plays an important role in informing the UN processes by providing feedback on the practical implementation of UN recommendations.

Practical implementation of the CBMs

2023 marked the tenth anniversary of the adoption of the first set of OSCE cyber/ICT security CBMs. The OSCE launched a publication which serves as a collection of OSCE experience in the development and implementation of such measures, presenting examples of best practices and key results. It describes efforts across the OSCE area and highlights key examples of the OSCE Secretariat's work in the field and includes information on publicly available resources, such as e- learning courses and good practice reports. https://www.osce.org/secretariat/5559ww99

For more information please visit:
https://www.osce.org/cyber-ict-security

Contact

OSCE Secretariat
Transnational Threats Department
cybersec@osce.org

Innovations – A competitive advantage

Innovations should not only be promoted, but also precisely managed and made measurable – as part of our corporate culture. Innovation is central to Saab's future.

Increasing cooperation within Europe – at EU level (for example through EDIRPA, the instrument used to strengthen the European defence industry through joint procurement) as well as within NATO (for example through the Defence Production Action Plan DPAP) – is strengthening the strategic autonomy of the European defence industry. This entails responsibility and requires a targeted expansion of capacity.

Saab takes this task seriously and is continuing to invest heavily in research and development: in 2024, around 17 per cent of turnover was invested in R&D. Saab is constantly working on adapting products and services to changing requirements and customer needs – with the aim of always remaining one step ahead. The coming years will be dominated in particular by software-based technologies, autonomy and AI-supported functions. As a comparatively small global player, Saab learnt early on how to innovate in terms of system design, speed of response, and cost and performance efficiency.

A future with partners

Many ground-breaking technologies – such as artificial intelligence or unmanned systems – are now being developed outside of traditional defence companies. That is why Saab is increasingly focussing on strategic industrial partnerships in a wide range of markets in order to develop the best possible solutions for modern armed forces. Cross-industry cooperations and targeted acquisitions are also gaining in importance. The aim is to be able to grow locally and become an integral part of the respective defence ecosystem.

This strategy – combined with targeted acquisitions – allows innovations to be integrated quickly and efficiently into existing Saab systems. These include machine learning and generative AI in sensor and application systems to improve data analyses and decision-making. One example of this is the acquisition of BlueBear, which has expanded the company's expertise in the field of AI-based swarm technologies for air and sea domains.

Saab is also investing in the German company Helsing GmbH, a defence company specialising in AI software. Saab will benefit from the close cooperation with Helsing with state-of-the-art capabilities being implemented across the portfolio. The cooperation will begin in the areas of electronic warfare and reconnaissance capabilities for fighter aircraft as well as other sensors and command and control applications in all domains.

> **"We are open to new trends and technologies and are constantly monitoring them so that we can offer our customers new opportunities."**
>
> Ellen Grev, President Saab Emerging Technologies

This consistent innovation strategy not only makes Saab a sought-after partner for armed forces customers worldwide, but also secures the company a dominant position in the increasingly technology-driven defence environment.

Saab is a leading defence and security company with an enduring mission: to help nations protect their people and society. With the help of 25,000 talented employees, Saab is continuously pushing the boundaries of technology to create a safer and more sustainable world. Saab develops, manufactures and maintains advanced systems in the fields of aviation, weapons, command and control systems, sensors and underwater systems. Saab's headquarters are located in Sweden. The company operates globally and is part of the national defence structure of several countries.

saab.com

VCDNP
Vienna Center for Disarmament and Non-Proliferation

Efforts by the VCDNP on AI and nuclear security in 2024 and 2025

The Vienna Center for Disarmament and Non-Proliferation (VCDNP) was established in 2010 at the initiative of the Austrian Foreign Ministry as an international non-governmental organisation. The Center has a growing programme of work on emerging technologies, with a particular focus on artificial intelligence (AI) and security of facilities and activities using and storing nuclear and other radioactive material, and has undertaken a number of activities in 2024 and 2025.

In January 2025, the VCDNP hosted a workshop on security risks and opportunities for the nuclear supply chain related to the use of AI, involving representatives from national regulators, academia, industry, research institutes, and international organisations. The workshop explored how AI technologies can impact the security of the nuclear supply chain, whether in the hands of malicious actors or used beneficially for applications in the nuclear sector.

Drawing on the discussions in this workshop, VCDNP published an expert report in April 2025 authored by Dr. Sarah Case Lackner and Ms. Mara Zarka, entitled "Nuclear Security and the Security of the Nuclear Supply Chain in the Age of Artificial Intelligence", highlighting the risks and potential benefits that AI could bring to the nexus of nuclear security and the nuclear supply chain. The report's key takeaways were presented during a hybrid event in April 2025.

A second publication focusing on nuclear security was also released as a joint publication by VCDNP and AIT (Austrian Institute of Technology) in April 2025, authored by AIT-affiliated expert Mr. Donald Dudenhoeffer, entitled "Past, Present, and Future Applications of AI in the Nuclear Sector". The paper provides a summary of current and future AI applications in the civil nuclear sector ranging from reactor design and defect detection to predictive maintenance and disaster response. The paper is the first product of a partnership between the VCDNP and AIT and includes a joint foreword by Dr. Helmut Leopold, Head of the AIT Center for Digital Safety & Security, and VCDNP Executive Director Elena K. Sokova.

Two further papers discussing the intersection of AI and nuclear security were also released in April 2025: "Counterfeiting, Artificial Intelligence, and Supply Chains in the Nuclear Sector" by Prof. Christopher Hobbs and Ms. Zoha Naser of Kings College London, which presents new insights on how AI could raise nuclear safety and security risks by facilitating the insertion of counterfeit, fraudulent, and suspect items across the supply chain for nuclear facilities; and "Artificial Intelligence, Nuclear Security, and the International Legal Framework" authored by Dr. Anita Nilsson, which maps international governance instruments on nuclear security and their ability to address AI-driven risks and threats.

VCDNP experts also provided briefings on AI and nuclear security at various fora in 2025. Furthermore, a seminar including AI topics was convened by VCDNP in January 2025 on "The Impact of Emerging Technologies on the Nuclear Supply Chain".

In addition to this work on AI and nuclear security, the VCDNP has also sought to raise awareness within the Vienna diplomatic community on risks and challenges at the intersection of AI and weapons of mass destruction (WMD). These efforts have included a special session on AI at the annual diplomatic workshop for Vienna ambassadors and heads of international organisations in June 2024, as well as three seminars for Vienna diplomats: "Generative AI and Non-Proliferation" in February 2024; "Generative AI in Diplomacy and WMD Non-Proliferation: Navigating Opportunities and Challenges" in September 2024; and "Advances in Artificial Intelligence and its Impact on Nuclear Issues" in January 2025.

The VCDNP is now initiating a new project focused on the intersection of the Internet of Things, AI, and nuclear security, expected to result in an expert report at the end of 2025.

Contact

Sarah Case Lackner, Ph.D.
Senior Fellow

Vienna Center for Disarmament and Non-Proliferation (VCDNP)

scaselackner@vcdnp.org
+43 (1) 236 94 82

VICESSE Research – Vienna Centre for Societal Security

VICESSE focuses on the analysis of a wide array of security issues in a broad societal context. We locate security problems emerging at local, national and European levels in wider social and historical contexts. Conceiving of security as a societal concept, we strive to integrate and combine different analytical perspectives into a complex framework providing the basis for rigorous empirical and theoretical academic studies and pragmatic policy solutions alike. Our mission statement is to bring security back into society. This entails a dual task: linking contemporary security solutions to the everyday world of citizens and giving members of society a critical voice in security research.

Selected Research Fields and Projects

Artificial Intelligence

Trustworthy AI
Development of criteria and a certification process to evaluate trustworthy AI systems, focusing on ethics, safety, and fairness.

FairAlgos
Analysis of discrimination and bias in algorithmic decision-making, with the goal of creating quality criteria for fairness and transparency.

AlgoCare
Investigates the use of AI in long-term care settings, particularly issues of algorithmic bias and the application of explainable AI (XAI) to foster trust and transparency.

KiMeGe
Analysis of the societal impacts of AI, including the risks and threats posed by AI.

Cyber Security

CSKA
Strengthen cybersecurity capabilities in Austria. In light of increasing cyber threats, new EU regulations, and rapid technological change, CSKA captures and analyses the current and future labour market situation in the field of cybersecurity.

CONTAIN
Researches technical, procedural and organisational measures to reduce the reduce the impact of cyber-attacks on supply chains and increase the increase the resilience of partners.

Technology & Societal Impact

iBOT4CRMs
Investigation on how advanced AI, robotics, and data science can be utilized for sustainable management of critical raw materials (CRMs), with a focus on the impact of technologies on organisations and workers.

DISRUPT
Improving the fight against child trafficking, by enhancing the use of digital evidence in investigations and prosecutions. It seeks to reduce victims' exposure to retraumatization while strengthening cross-sector collaboration and professional capacity across Europe.

Further Research Fields

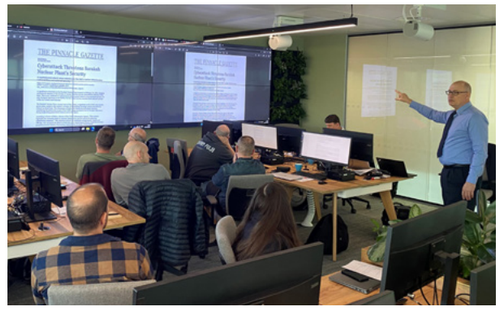
Domestic Violence, Data Protection, Incarceration, Infrastructure, Crisis Management, Justice System, Organized Crime, Policing, Sociology of Law, Theory of Society

Contact Details

Maintaining safe and secure energy supplies: Cybersecurity for Nuclear Industry professionals

Energy security and electric power production are essential pillars of a stable society. The rapid pace of digital transformation, the widespread adoption of advanced technologies, and the increasing global demand for electrical power underscore the need for reliable, resilient, and safe and secure energy generation. Among the available options, nuclear energy stands out as the most effective solution for delivering sustainable, non-carbon power.

Protecting power generation and other critical infrastructure from cyberthreat actors from. Power generation facilities and other critical infrastructure remain prime targets for cyberattacks. While advanced technologies like Artificial Intelligence offer promising innovations and benefits, they also provide cyberthreat actors with tools to develop more sophisticated cyberattacks. As cyberthreat evolves, the importance of cybersecurity program management and development is essential to maintain strong defences and resilience to protect digital assets in Information Technology (IT) systems and Operational Technology (OT) systems.



Delivery at Lancaster University 2025. Source: WINS

A Global Training Initiative for Strengthening Nuclear Cybersecurity
The World Institute for Nuclear Security (WINS) offers a comprehensive five-day training course designed to equip nuclear industry professionals with the latest expertise and practical tools for developing and managing robust cybersecurity programmes. Covering data security, IT, and OT, this course blends operational experience with cutting-edge best practices to ensure the effective implementation of cybersecurity within nuclear facilities.

Developed in collaboration with the Austrian Institute of Technology (AIT), this flagship course has been successfully delivered worldwide over the past three years. It has supported a diverse array of nuclear security stakeholders, ranging from well-established civil nuclear programs to emerging initiatives exploring nuclear new-build opportunities. Industry-leading instructors bring real-world experience to the training, ensuring that the course can be tailored to meet the specific capacity-building needs of individual organisations, countries, and regions

"The training equips participants with tools to face evolving cyberthreats, delivered by nuclear security experts with cutting-edge cyber intelligence."

The course provides a dynamic and comprehensive cybersecurity training experience with a balanced mix of 60% lecture and 40% hands-on exercises, fostering an active and engaging learning environment. It is designed to immerse participants in practical applications while ensuring a deep understanding of cybersecurity principles within the nuclear sector, including cyber risk management and vulnerability assessment of cyberthreat to nuclear facility IT and OT system digital assets and having in place processes and systems for prevention, detection and response to threats, and maintaining safety and operational integrity of physical processes.

Building upon established technical standards—including ISO 27000, IEC 62443, NIS, and NIST—the course is uniquely tailored to address the specific challenges of the nuclear industry. It integrates expertise from leading organisations such as the IAEA, NEI, USNRC, and other key stakeholders in nuclear security, ensuring the application of industry best practices in guideline implementation.

The course is highly relevant to a broad spectrum of professionals, ranging from Chief Information Security Officers (CISOs), cybersecurity specialists and nuclear facility engineers to nuclear policymakers and regulators. In addition to covering the technical aspects of cybersecurity program management, the training takes a multidimensional approach, incorporating critical topics such as insider threat mitigation, security by design, supply chain security, and crisis management. This comprehensive framework ensures participants are equipped with the knowledge and skills needed to enhance nuclear cybersecurity resilience.

"This training is essential for staying ahead of rapidly changing cyberthreats. It helps professionals build the technical and strategic know-how needed to protect nuclear facilities and infrastructure," said Roland Fletcher, Head of WINS Certification and Training. "Our collaboration with AIT and Lancaster University ensures the course is grounded in both academic insight and practical application."

Upon completion, participants will be prepared to pursue and schedule the independently proctored exam to be awarded the prestigious WINS Academy Cybersecurity Nuclear Professional Certification and Digital Credential.

2025 Remaining Course Schedule
- Lancaster University, Lancaster UK, 15–19 September 2025 at (£2875.00 per delegate)
- AIT Austria Institute of Technology, Vienna Austria, TBD November 2025 (details TBD)
- Others as arranged/per request.

If you are interested in attending the training at Lancaster, Vienna, or arranging a course in 2026, please contact info@wins.org

ABA INVEST WORK FILM
Your easy access to Austria

Austria – Great Place to Launch your Cybersecurity Business

Austria's cybersecurity market is expanding rapidly, driven by strong demand from the public sector, critical infrastructure, industry, and private companies. The country has emerged as a recognized hub for cybersecurity, with growing numbers of firms and significant investment in research.

International organizations like the OSCE and IAEA, both based in Vienna, work closely with the Austrian Institute of Technology (AIT) on cybersecurity topics, including the protection of nuclear infrastructure.

One key factor behind Austria's appeal is its skilled talent pool. Over 30 % of university graduates hold degrees in STEM subjects. Austria ranks third in the EU for research intensity, with R&D spending at 3.35 % of GDP.

To support innovation, Austria offers a 14% research tax credit—uncapped—for all R&D-related expenses, including R&D staff, research infrastructure, financing and operational costs. Also contract research is encompassed.

Austria focuses on education: around one-third of students graduate in STEM fields, placing Austria second in the EU regarding number of STEM graduates per capita. And Labor productivity is 14.2 % above the EU average.

Excellent support – free of charge!

The Austrian Business Agency offers personalized assistance to companies looking to set up or expand in Austria. The INVEST in AUSTRIA team provides ongoing support before, during, and after market entry.

We deliver clear, concise information to reduce complexity and help you make the decision for Austria as your business location. Services include:

- Market and industry insights
- Site search assistance
- Contact building and networking
- Company setup guidance
- Funding and financing advice
- Talent pool access

Interested in learning more?
Find us at the expo area, or contact us:

CYBER RANGE
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

AIT Cyber Range – Training Center

AIT's Cyber Range is a virtual environment for flexible simulation of critical IT and industrial OT systems with complex networks, different system components and users. It provides a secure and realistic environment for analysing and testing incidents in various scalable scenarios without using real production systems. This allows different security processes to be rehearsed for live operation and special incident response processes for cyber incidents to be tested, in order to meet the highest security requirements for system architectures and operating processes. The AIT Cyber Range training courses and exercises address the cyber security needs of staff, IT professionals, CERTs/CSIRTs, management and advisory boards in industry, research and government. Beside using the Cyber Range in the academic sector for education it is used for global cyber security trainings for the nuclear sector as well as for governmental cyber security exercises.

THE AIT CYBER RANGE SUPPORTS

Training
Cyber security training for increasing cyber security capabilities of staff (from general staff to managers) in organizations.

Exercise
Hands-on experience on incident management and response for staff, CERTs/CSIRTs in a simulated virtual environment.

Research
Cyber security research on infrastructures and scenarios that are needed to maintain resilience of organizations.

Development
Secure development of software related to incident management and cyber security.

The AIT Cyber Range was developed by AIT in a strategic cooperation with the IAEA International Atomic Energy Association. Today, the AIT Austrian Institute of Technology operates as worldwide first IAEA Collaborating Centre in the field of cyber security for nuclear safety in IAEA´s member states.

In addition, the AIT, together with the Competence Centre Secure Austria (KSÖ), regularly conducts state-of-the-art cyber range training with authorities, companies and operators of critical infrastructures.

Further Information

https://cyberrange.at

Contact

Mag. (FH) Michael Mürling, MA AI4Gov
michael.muerling@ait.ac.at

Fake-Shop Detector

Fake-shops cause significant economic damage; a dark field study estimates that 320,000 consumers in Austria are directly affected and puts the damage at €16 million. The Fake-Shop Detector (FSD) is an open source project from AIT and a free service that warn of fraudulent online retailers directly in the browser, proactively and effectively protecting Austrian consumers when shopping online. The detector uses over 26,700 known fake shops (blacklist) in German-speaking countries. In addition, the Detector uses artificial intelligence (AI) to analyse unknown websites in real time and assess their similarity to known fraudulent sellers.

It is not individual features that are decisive in calculating the threat potential, but a large number of features in combination. More than 22,000 features are included in the real-time risk assessment using AI. Over the last 3 years, more than 1.9 million web shops have been evaluated and analysed by the Fake-Shop Detector's AI, achieving a model accuracy of over 91% in practical use. Another key feature of the FSD is its manual quality assurance, which is carried out by Watchlist's internet experts on an ongoing basis. This is particularly important as the FSD is a security-related service aimed at consumers who need to be protected when shopping online.

The result of the Fake-Shop Detector analysis is displayed using a traffic light system. A red symbol warns of known fake shops and the suspicious shops recognised by the AI.

The tool was developed by a team, consisting of the AIT Austrian Institute of Technology, the Austrian Institute for Applied Telecommunications (ÖIAT) and the IT specialist X-Net. In November 2024, AV-Comparatives conducted a comprehensive Fake-Shops Detection Test, which evaluated the effectiveness of various cybersecurity solutions in identifying fraudulent e-commerce websites. In this test, FSD outperformed 35 international cyber security products that were tested for their effectiveness against counterfeit stores. In early 2025 the FSD received certification for its fake shop detection capabilities, highlighting its commitment to user safety and security.

Further information

Fake-Shop Detector Website and Download
https://fakeshop.at

Prizes and Awards

- ACR Innovation Award 2020, https://www.acr.ac.at/awards/innovationspreis-2020/fake-shops-aufspueren/
- eAward 2023 https://www.report.at/award/22888-eaward-2023-grosse-bandbreite-an-it-themen
- Nominated for Houska Prize 2023 https://bcgruppe.at/project/fake-shop-detector-der-ki-echtzeitschutz-fuer-konsumentinnen/
- State Prize for Digitalization 2024 https://www.konsumentenfragen.at/konsumentenfragen/Aktuelles/Konsumentenfragen/Staatspreis-Digitalisierung-fuer-richtungsweisenden-Fake-.html
- Constantinus Award 2024 https://www.constantinus.net/wall-of-fame/57662.html/
- The FSD was rated by AV Comparatives in August 2024 as the most effective security product against fake online stores. https://www.av-comparatives.org/tests/fake-shops-detection-test-november-2024/

Funding schemes

Innovation enabled by public funding programmes:

- KOSOH (KIRAS) https://www.kiras.at/gefoerderte-projekte/detail/d/kosoh
- MAL2 https://www.malzwei.at/
- INSPECTION (German Federal Ministry of Education and Research as part of KMU Innovativ) https://www.mindup.de/data-scientists/anwendungsfaelle/fake-online-shops.
- DETECT (netidee) https://www.netidee.at/detect.
- SINBAD (KIRAS Security Research Programme) https://projekte.ffg.at/projekt/3807747
- RIO (KIRAS Security Research Programme) https://projekte.ffg.at/projekt/4489816

Contact

Mag. (FH) Michael Mürling, MA AI4Gov
michael.muerling@ait.ac.at

AIT Media Intelligence Platform

At the AIT Austrian Institute of Technology, Center for Digital Safety & Security, Competence Unit Data Science & Artificial Intelligence, tools are being developed to support human experts in better identifying DeepFakes and manipulated or AI-generated media content.

The topic Media Intelligence is concerned with algorithms and technologies that make it possible to analyse and interpret multimedia content such as images, videos, audio files and associated texts, and to make the information and obtained results.
For example, computer vision techniques are applied to the development of methods for automatically recognizing and classifying objects in images and videos. These methods are used to evaluate the authenticity of multimedia content based on various indicators (e.g., manipulation of images or audio, detection of deepfakes or synthetic media).

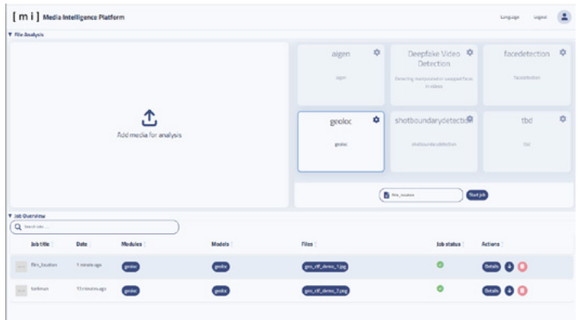
In addition to the analysis of audiovisual characteristics, methods of Natural Language Processing (NLP) and Explainable AI (XAI) are also applied. These enable the automatic classification and evaluation of text-based content that is linked to multimedia content. For example, image and video subtitles, social media posts, comments or metadata can be analyzed to draw conclusions about the plausibility, origin and possible manipulation or contradictions of content. By combining computer vision, NLP and XAI, multimodal misinformation, for example, can be better recognized, understood, and contextualized.

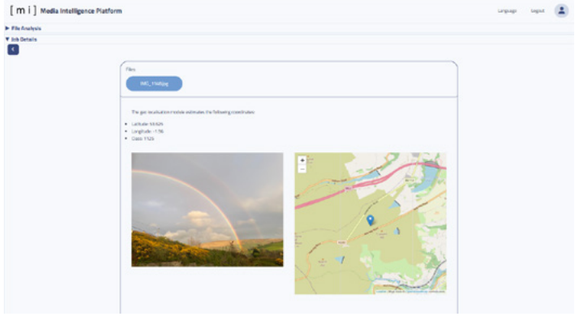
Furthermore, methods for context enrichment are used to compare media content with additional information (e.g., place of recording, temporal inconsistencies, source information). This enables a well-founded check for disinformation or targeted manipulation.

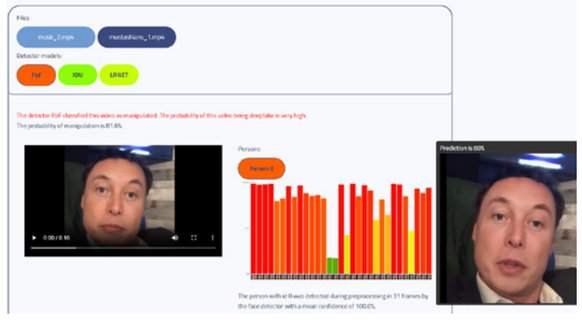
The modular and scalable design of the methods makes it possible to process large data collections efficiently in our Media Intelligence Platform. This is particularly relevant for applications in the fields of digital forensics, combating disinformation, terrorism prevention, and open-source intelligence and supports the analysis of media content by fact-checkers, security authorities, and law enforcement.

Contact

Mag. (FH) Michael Mürling, MA AI4Gov
michael.muerling@ait.ac.at







AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AIT Quantum Cryptography

One of the most important methods for improving data protection and combating cybercrime is the encryption of data. A central problem here is the generation of key material for efficient and secure communication. Quantum physics helps in this regard, for example, with the phenomenon of “entangled particles”: two entangled light particles (photons) have exactly the same properties, even if they are very far apart. If the properties of one of the two particles are measured, this has a direct effect on the other particle. On the one hand, this means that you can generate completely random bit sequences - a cryptographic key - at two different locations. On the other hand, it also means that you immediately know when someone is trying to listen in, as the very act of reading out information changes the state of the particles concerned.

Around 25 years ago, the Viennese quantum physicist Anton Zeilinger (University of Vienna, Austrian Academy of Sciences ÖAW) demonstrated that this principle of quantum key distribution (QKD) can be used in practice for the transmission of information. In 2004, for example, a symmetric key was transmitted by means of entangled photons via a 600-metre-long fiber optic cable between a Viennese bank and the city hall. Since then, this has also been achieved in fiber optic networks hundreds of kilometers long, between two Canary Islands, between different countries and even via a satellite between Beijing and Vienna. For this pioneering work on quantum physical entanglement, Zeilinger - together with his colleagues John Clauser and Alain Aspect - was awarded the Nobel Prize in Physics in 2022.

Researchers from AIT Austrian Institute of Technology have been involved in Zeilinger’s experiments from the very beginning. They develop the technical equipment for quantum cryptography as well as the necessary software and organize large European research networks. Over the years, the AIT has built up an international and excellent reputation as a specialist in both terrestrial and satellite-based quantum cryptography and as a mediator between the various scientific disciplines of quantum optics, photonics, post-quantum cryptography and cyber security, thus driving forward key implementation initiatives for a secure, networked Europe as a leading international competence center for quantum technology. Today, the AIT is a key player in major EU projects as part of the EuroQCI initiative (European Quantum Communication Infrastructure Initiative) launched in 2019, which funds the development of QKD networks and concrete testbeds in Europe with the aim of strengthening Europe’s data sovereignty. In this context, AIT is part of large EU-funded projects (QCI-CAT, PETRUS, NOSTRADAMUS, QOSILICIOUS, OpenQKD, UNIQORN, CiViQ, QUARTZ, QSAFE, etc.) and received also funding from the Austrian Security Research Program KIRAS (e.g. QKD4Gov).

An important research focus is currently on the miniaturization of the devices required for quantum communication. To this end, hardware is being developed that has the same functionality as previous large laboratory setups, but is integrated on an optical chip. The aim is to create small and compact end devices that can be easily used by all users with a fiber optic connection - similar to a modem for Internet access on a computer today. As early as 2023, a miniaturized QKD transmitter with a photonically integrated chip that combines all components such as lasers, modulators and attenuators in a very small space was presented at Europe’s largest IT security trade fair “it-sa”.

In addition to the development of terrestrial quantum communication networks, research activities are also focusing on another important area - space. Thanks to the almost unlimited coverage via satellites, the current restrictions on transmission via fiber optic-based QKD systems - which limit transmission ranges to a few hundred kilometers - can be overcome and a globally available quantum-secured cyber security solution can be installed for remote regions in the future. The future encrypted EU satellite network IRIS2 also relies on EuroQCI. The European satellite constellation aims to provide governments with highly secure communication services and to network critical infrastructures in a highly secure manner. After Galileo for navigation and Copernicus for earth observation, IRIS2 is the third pillar of the EU space infrastructure.

“Our strong position in the major EU programs for quantum communication is the result of years of fundamental development at the AIT, which was significantly supported by Austrian research funding programs. In particular, the KIRAS security research program and the Quantum Austria research program served as a real launch pad for EU projects.”

Martin Stierle,
Head of Competence Unit Security & Communication Technologies

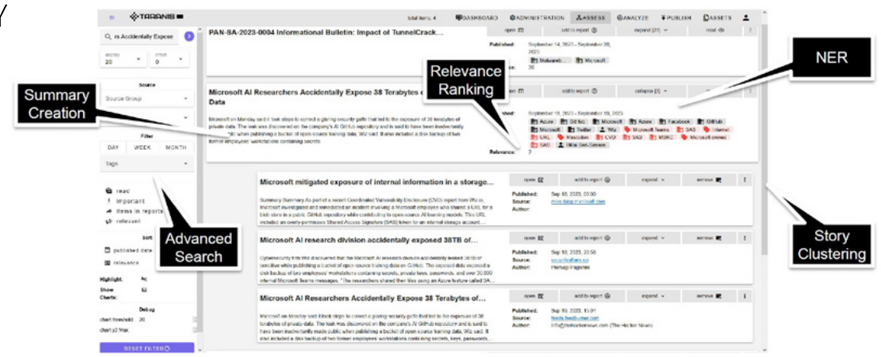
Further information

https://www.ait.ac.at/quantum
https://www.kiras.at/en/financed-proposals/detail/qkd4gov
https://qci-cat.at
https://petrus-euroqci.eu
https://qt.eu/ecosystem/quantum-communication-infrastructure

Contact

Mag. (FH) Michael Mürling, MA AI4Gov
michael.muerling@ait.ac.at

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY



Taranis – AIT OSINT Cyber Security Open Source Project

Taranis AI is an advanced Open-Source Intelligence (OSINT) tool from AIT, that leverages Artificial Intelligence to revolutionize information gathering and situational analysis.

Open-source intelligence (OSINT) provides up-to-date information about new cyber-attack techniques, attacker groups, changes in IT products, updates of policies, recent security events and much more. Often dozens of analysts search a multitude of sources and collect, categorise, cluster, and rank news items from the clear and dark web in order to prepare the most relevant information for decision makers. A tool that supports this job is “Taranis NG” from the Slovakian CERT. This solution ingests information from many types of sources such as websites, RSS feeds, emails and social media channels and makes them searchable. It also supports the creation of reports and daily summaries. However, the number of sources and news items is continuously growing, making it increasingly difficult to search them purely manually. These circumstances call for the application of novel natural language processing (NLP) methods to make OSINT analysis more efficient.

Gathering mostly public information is essential to maintain situational awareness and take early actions in security matters. Large organisations, national authorities, and analysis centres collect on a wide scale potentially hundreds of sources with thousands of articles daily, and analyse them for relevant content to create so-called products, which are essentially reports for certain constituencies that support decision-making processes. It is obvious that the quality of these reports highly depends on the level of sophistication of the analysis phase.

However, ingesting, analysing and making use of semantically richer “soft” Cyber Threat Intelligence (CTI) is much more demanding than ingesting well-structured machine-readable technical CTI. This soft CTI usually comes as unstructured freeform text, containing high-level, often ambiguous strategic information designed for human consumption – and indeed, in course of complex analysis workflows is usually consumed by human analysts only. This is tedious, resource-intensive, and error-prone work. As the number of OSINT sources as well as the frequency of published articles rises, we need new analysis techniques to keep pace with these developments and to not miss any critical pieces of information. Luckily, natural language processing (NLP) and Artificial Intelligence (AI) have made tremendous progress in recent years.

In the course of our research, we explore five essential user stories together with our stakeholders from national authorities and CERTs that human OSINT analysts face in their daily work. Supporting these user stories with appropriate technical means is the goal of Taranis AI:

- User Story 1: What was going on in the cyber security domain in the last 24 hours? (“Hot Topics Clustering”)
- User Story 2: What do we know about a specific entity? (E.g. a vulnerability, malware, company, product, person, etc.)
- User Story 3: I‘ve read an interesting article. What further related news items exist?
- User Story 4: Which news items are recommended for me based on my recent preferences (collaboratively and AI-assisted)?
- User Story 5: I‘d like to build a report for certain clients. How to sum up my findings efficiently?

Project Taranis AI

The CEF project AWAKE and EDF-funded projects NEWSROOM and EUCINF explore how Taranis NG can enhance cyber situational awareness using data from the clear and dark web. They focus on integrating modern NLP into Taranis AI to classify news, extract entities, and group related items into “stories” that highlight key topics and reduce analyst workload. Additional features include auto-generated summaries and a collaborative ranking system. Taranis AI is open source and available under the EUPL.

Further Information: https://taranis.ai/

Contact

Mag. (FH) Michael Mürling, MA AI4Gov
michael.muerling@ait.ac.at

Diplomatic Insight Group
Innovative Diplomacy for Peace, Security, and Digital Cooperation

Diplomatic Insight Group is pioneering an innovative model of hybrid diplomacy that integrates strategic communications, digital engagement, and policy-focused research.

Platforms at the heart of our system include:

- The Diplomatic Insight Magazine (since 2008), a trusted source of analysis for diplomats and policymakers;
- Institute of Peace and Diplomatic Studies, a think tank focused on peace diplomacy, hybrid threats, and public policy innovation;
- DiploTV, a YouTube channel focusing on digital diplomacy and strategic communications.
- Global News Pakistan, the country's first multilingual newswire service;

As a woman-led and owned network operating at the intersection of diplomacy and technology, our initiatives respond directly to the challenges and opportunities for diplomats, policymakers, scholars, and citizens.

We offer real-time insights, curated analysis, and engagement tools for our audience, providing multilingual content, strategic briefings, and issue-specific forums.

What We Seek at IDSF

Our goal is to build new interregional partnerships around digital diplomacy, civic resilience, and soft power strategy. We welcome dialogue with institutions interested in co-developing:

- Joint foresight platforms and research hubs
- Communication strategies for risk analysis and diplomacy
- Training & fellowship exchanges on strategic communications, foreign affairs, and international security

Our work is rooted in trust, diversity, and local-global linkages. At a time when the Global South is stepping forward as a co-shaper of norms, DIG represents a credible, tested model of innovation in diplomacy from one of the world's most complex yet consequential regions.

More at

www.thediplomaticinsight.com
www.ipd.org.pk
www.diplomaticinsightgroup.org

About us

fragmentiX Storage Solutions is an Austrian cybersecurity company, producing quantum-safe storage appliances. Using Secret Sharing technology it enables secure decentralized data storage in the cloud.

Project

CVSTAR
In the applied research project CVSTAR, that is coordinated by the Technical University of Denmark (DTU), we have researched and implemented two proof-of-concepts for fragmentiX products: (i) distributed cryptographic storage self-healing against malicious attackers and (ii) quantum-safe link encryption using keys retrieved through an ETSI GS QKD 014 compliant interface from QKD systems without the need for external link encryptors. These two features will be tested in network demonstrations at the DTU and the Danish network operator TDC NET in May and June 2025. QuantERA CVSTAR has received funding from FFG.
(Project ID: FO999891361)

QUARTER
In the project QUARTER, that is coordinated by the Spanish QKD manufacturer LuxQuanta, we are redesigning and developing the next generation of our leading product, the fragmentiX CLUSTER NODE. It features a quantum random number generator as physical entropy source, and the cryptographic storage self-healing and quantum-safe link encryption studied in CVSTAR. It will be demonstrated in a use-case at Telefónica during 2025. QUARTER has received a funding from EU.
(Project ID: 101091588)

SAGA
In SAGA (Security And cryptoGrAphic mission of the European Space Agency) which forms an important part of EuroQCI fragmentiX is involved in proofing the security of the space QKD system. SAGA 2 has received a funding from EU.

QCI-CAT Use cases
fragmentiX is involved in two usecases within the project QCI-CAT, the Austrian contribution to EuroQCI with the goal to develop a Europe wide quantum communication infrastructure.

Government use case
In the governmental usecase, four Austrian ministries are equipped with fragmentiX CLUSTERs, storage servers and QKD devices in order to implement a federated storage and data distribution solution. QCICAT has received a funding from EU and FFG.
(Project ID: 101091642)

Medical use case
In the medical use case, a blueprint for a distributed data repository for highly sensitive medical data is created, using fragmentiX secret sharing technology. To overcome the distance limitation of QKD devices, fragmentiX developed Trusted Repeater Nodes which are deployed to relay the signal from Graz to Vienna.

General

fragmentiX as a Service
In addition to the continuous improvement of their storage appliances fragmentiX – together with their longtime business partner connect4Video – is currently developing "fragmentiX as a Service". This is an easy-to-use solution that enables clients to utilise the security of fragmentiX without having to worry about integrating hardware.

ISO certification
In order to strengthen both the dynamically growing organisation and our commitment to information security, fragmentiX has started the process of ISO 27001 certification until the end of 2025.

Contact

Christoph Pacher
christoph.pacher@fragmentix.com
+43 677 631 00 148

EU Innovation Through EU Co-operation

Alone we can achieve a lot, together we can achieve everything!

Since 2001, ICSL has been committed to protecting classified communications—voice, video, data, and chat—at the highest level for the military, government authorities, and critical infrastructure providers.

Such achievements would not be possible without trusted partnerships across the EU—with manufacturers, developers, and, above all, our valued clients, whose feedback plays a vital role in the ongoing refinement of solutions that meet the demands of everyday use.

© iStock / Tom Merton

Custom Mobile COMSEC for Austria's Federal Government

Due to its unwavering commitment to confidentiality, ICSL rarely discloses client references—unless the client has made them public. A notable exception is the Austrian Federal Ministry of Defence (BMLV), which has officially documented its use of the solution in several annual reports. Already in 2020, the BMLV concluded a framework agreement with ICSL to deliver a customised version of the Silentel platform for secure communication across top-level government institutions.

"The version used by the Federal Government is a 'Custom App', identifiable by the federal eagle in the logo, which allows the BMLV as the system operator to retain full control over access and further development."
(BMLV Annual Report 2020, pp 82-83)

Approved for EINGESCHRÄNKT and EU RESTRICTED levels, the system ensures sovereign, centrally governed communication—beyond the reach of commercial messaging platforms.

Forward-Looking Security That Proves its Worth in Crisis

Brigadier Walter Unger, former Head of Cyber Security at Austria's Military Intelligence Service, explains in an interview with Die Presse why a „Signal-gate" incident like the one in the United States could not have occurred with Austria's dedicated federal app.

"The difference with this app, compared to Signal, is that it is not publicly available and can only be used by a restricted group of users."

Unger also refers to a specific case from 2017, when several mobile phones were extracted for data after an accident—a scenario that, he notes, would have been prevented by the federal app:

"Had the Interior Ministry staff been able to use the federal app [which was not available at the time], the data would not have been readable: The app provides protection mechanisms for such cases."

As published in Die Presse, 27 March 2025, article:
"The App That Safeguards Austria's Secrets".
(Original title: „Die App, die Österreichs Geheimnisse schützt")

Contact

icsl.at
office@icsl.at
+43(1)33286-80300

European Cyber Defense in Practice: This Is What Digital Sovereignty Looks Like

Cyber threats know no national borders. Ransomware waves such as "WannaCry" or "NotPetya" have paralyzed networks worldwide within hours. Critical infrastructures — from hospitals and ministries to energy providers — are increasingly being targeted. Disinformation campaigns also regularly affect multiple EU countries in parallel.

This trend makes one thing clear: no country can protect itself alone. For Europe, digital solidarity is therefore a strategic lever to strengthen digital sovereignty, protect shared values, and ensure sustainable economic development.

What Does Cybersecurity Without Backdoors Mean?

Digital sovereignty refers to the ability to make independent decisions regarding digital infrastructure, data, and technologies — essential for independence and the protection of information. Using non-European security solutions carries geopolitical risks and leads to technological dependencies.

Sovereign cybersecurity therefore means having full control over the technologies used: through European development, transparency, open standards, and local data processing.

Digital solidarity, in turn, stands for shared responsibility: for exchange, harmonized standards, and interoperable technologies based on European values. It is the practical key to achieving digital sovereignty.

Stronger Together: A European Example from Practice

A European security solution for sovereignty and solidarity must be developed and operated in Europe and tailored to regional needs.

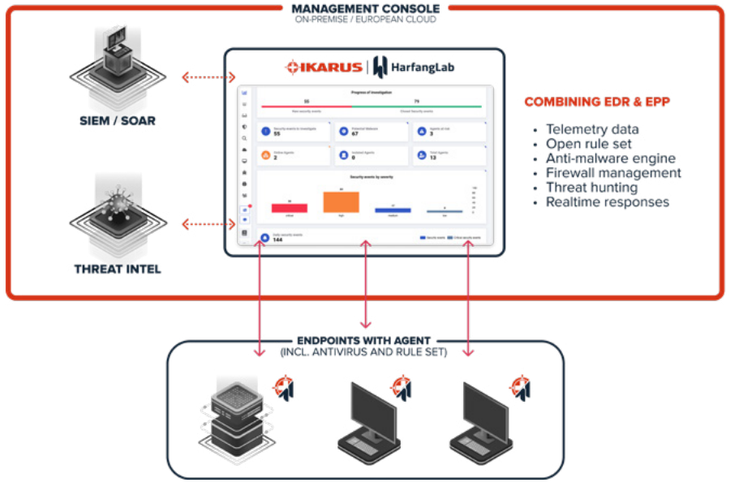
A concrete example is the collaboration between IKARUS Security Software (Austria) and HarfangLab (France). The jointly developed, ANSSI-certified EDR & EPP solution HarfangLab Guard feat. IKARUS offers:

- Fully European hosting (e.g., via IKARUS) or on-premises operation,
- Open YARA and Sigma rules for customizable threat detection,
- Disclosure of detection logic for maximum transparency,
- Air-gapped deployment for isolated environments without internet connectivity.

This architecture contributes to Europe's digital resilience — and represents a scalable model for further intra-European cooperation. It is an offering to public institutions, critical infrastructures, and technology-oriented companies to jointly place security in European hands.

Contact

sales@ikarus.at
+43 1 58995-500



IT:U Interdisciplinary Transformation University Austria

IT:U, the Interdisciplinary Transformation University Austria, is a new public technical university dedicated to digital transformation, driven by interdisciplinary research and project-based, personalized learning. This transformation is actively being shaped and advanced by IT:U with a solution-oriented approach.

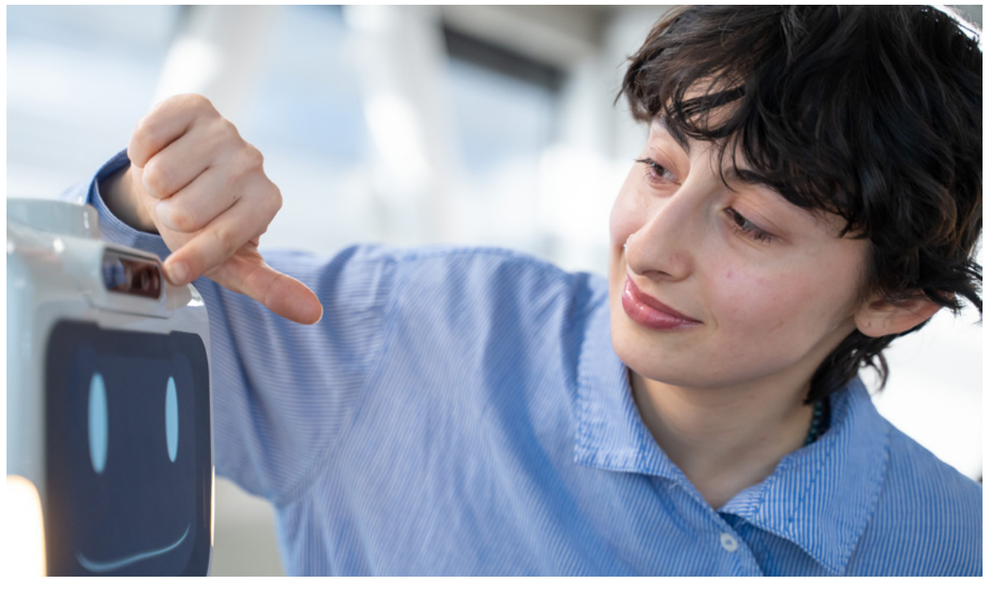
IT:U conducts interdisciplinary research and education at the intersection of Artificial Intelligence (AI) and fields such as medicine, sociology, psychology, and environmental engineering. The university focuses on applying digital technologies to address complex, real-world challenges across disciplines.

Its mission is to educate a new generation of Digital Transformers — professionals who combine deep subject-matter expertise with advanced digital skills to drive innovation in both research and industry. With a strong emphasis on inter- and transdisciplinary collaboration, IT:U offers mission-driven study programs and project-based learning that prepare students to navigate and shape the digital transformation of society.

The new Technical University for Digital Transformation comprises eleven research groups, which will be supplemented by further ten research groups by fall 2025. Amongst the new research areas will also be Cybersecurity, Quantum Communications and Quantum Cryptography. IT:U strives to connect to the European cybersecurity ecosystem.

Contact

Gerd Krizek
Senior Manager
Study Portfolio & Student Affairs
gerd.krizek@it-u.at



Stay up to date & follow!

CTI – Cyber Threat Intelligence – Qualification Network

With increasing cyber threats and evolving EU regulations like NIS2 and the Cyber Resilience Act, CTI is key to strengthening organizational security. A new qualification network led by SBA Research, with partners from academia and industry, delivers hands-on CTI training in six modules. The program focuses on open-source tools, automation, and threat analysis, aiming to boost cyber resilience, regulatory compliance, and digital sovereignty across Austrian companies.

ASOC – Academic Security Operations Center

The KIRAS project ASOC explores rapid, automated exchange of security information, IOCs, playbooks, and SOAR workflows to strengthen cybersecurity across Austrian universities. Led by SBA Research and partners, the project develops concepts for a federated, open-source academic SOC infrastructure, supports AI-driven threat hunting, and addresses legal, social, and educational aspects—boosting proactive defense and collaboration.

dAIbetes

The Horizon Europe project dAIbetes aims to develop privacy-preserving, personalized prediction models for treatment outcomes in type 2 diabetes. By using federated learning and virtual twin technologies, the project enables data-driven insights without compromising patient privacy under GDPR. This cross-national effort brings together experts in AI, cybersecurity, and diabetes care. SBA Research leads the work on data security, privacy, and model explainability. Building on the success of the FeatureCloud project, dAIbetes seeks to revolutionize personalized diabetes treatment through secure, federated health data platforms.

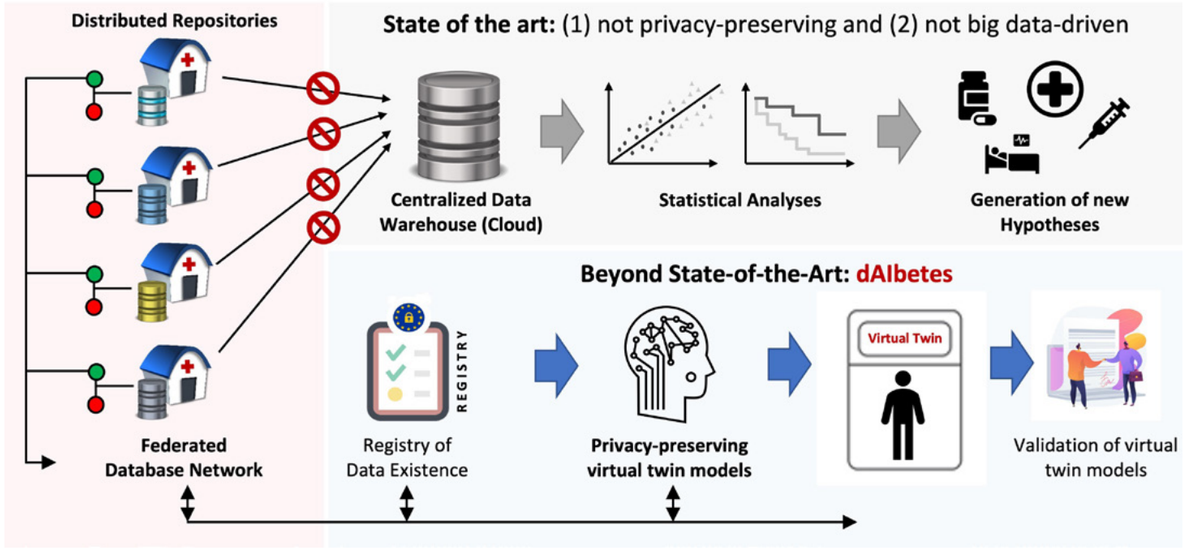
Contact

CTI / ASOC

Alexander Szönyi
aszoenyi@sba-research.org

dAIbetes

Rudolf Mayer
rmayer@sba-research.org



University for Continuing Education Krems

The Department for Security Studies (DSI) – Secure. Digital. Resilient.

Security – it is one of the most fundamental human needs. Without it, there is no basis for trust, cohesion and progress. In a world characterized by crises, global upheaval and technological upheaval, security is more than ever the focus of social attention. But what does security mean today – and for whom? Our work sees itself as a bridge between scientific knowledge and practical application. We show how the understanding of security is changing – and what this means for institutions, the economy and people's everyday lives. Because security is not just a subject of research – it is a shared task.

www.donau-uni.ac.at/dsi

Close connection between science and practice

The study cources **in the area of Security and Safety Management, Fire Safety Management, Information Security Management, Cybersecurity, AI and Counter-Terrorism, Prevention of Violent Extremism and Intelligence** are designed to be practice-oriented and linked to current research. Many lecturers come directly from practice and offer valuable networks as well as direct applicability in everyday working life. The university's courses are aimed specifically at mid-career specialists and managers who are looking for professional development, self-fulfilment at work or a new direction.

Mission

Our goal is to contribute to a safe and sustainable society through interdisciplinary research, innovative teaching and practical solutions.

"Security is as diverse as society itself. Globalization, terror, migration, AI and digitalization are changing structures and creating uncertainties. Solutions require trust and constructive dialog."

Walter Seböck,
Head – Department for Security Studies

Contact

Mag. Dr. Ingeborg Zeller
Deputy Head and Scientific Staff
Department for Security Studies
ingeborg.zeller@donau-uni.ac.at
Phone: +43 2732893 2316 / +43 664 8340033

University for Continuing Education Krems
Department for Security Studies
Dr.-Karl-Dorrek-Straße 30
3500 Krems
Austria

wirtschaftsagentur wien | Für die Stadt Wien

Kofinanziert von der Europäischen Union

Cybersecurity in focus: funding, advice and insights from Vienna

The Vienna Business Agency is intensively involved in the area of cybersecurity and supports Viennese companies with various offers to strengthen their digital security. A central component is the "Digitalization" funding programme, which is aimed specifically at small and medium-sized enterprises (SMEs). It promotes investment in new digital technologies, including IT and cyber security measures. Companies can receive up to 50,000 euros per project, with up to 50 % of the eligible costs being covered. In addition to financing, consulting services as well as training and further education measures in the field of digitalization are also eligible for funding.

The Vienna Business Agency also offers free individual consultations on digital technologies. The focus here is on topics such as cloud computing, artificial intelligence, mobile technologies and, in particular, cybersecurity. The Vienna Business Agency supports companies in the development and implementation of their digital projects.

Another important contribution of the Vienna Business Agency to the topic of cybersecurity is the creation of a technology report on cybersecurity. This report highlights current technological trends, identifies relevant developments and provides a comprehensive overview of the growing cybersecurity ecosystem in Vienna. The report serves both as a source of information for interested companies as well as a strategic tool for the further development of Vienna as a location for digital security.

In addition to funding, consulting and publications, the Vienna Business Agency also supports professional exchange by participating in events. For example, it is actively involved in the International Digital Security Forum (IDSF). Such international conferewnces, like the IDSF, bring together experts from business, science and politics to discuss digital sovereignty and global cyber resilience as well as strengthening the cybersecurity businesses in Vienna.

Overall, the Vienna Business Agency pursues the goal of strengthening the digital competitiveness and security of Vienna's economy - through financial support, individual advice, strategic analysis and international networking.

Contact

Daniela Pieters, MSc
Technologie Services
pieters@wirtschaftsagentur.at

X-Net GmbH – sharing Innovation

Since 1999, X-Net has been committed to providing the latest technologies from the open source sector and supporting its customers with expert and personalized service. As an IT service provider and solution provider, X-Net supports customers in the areas of network management, hardware development, IT consulting, and IT security solutions and implements complex web applications and customized software solutions for companies and institutions of all sizes and in all industries. Many of our projects and subsequent products originate from research projects.

Sec³-System

Sec³ is a combination of software and hardware for cross-company digital communication and creates an infrastructure that establishes a uniform security and service standard across a machine manufacturer's entire product range and product generations. Thanks to its independence from individual technologies, Sec³ can be used to make any plant generation IoT-ready. The Security by Isolation (SBI) method, in which each system or even individual components of a system are operated securely and independently in their own separate networks, offers the highest possible protection against cyber threats and attack scenarios and takes data sovereignty to a new level. At the same time, Sec³ creates all the conditions necessary for machines and systems to be put into operation easily, for service and support activities to be handled efficiently, and for predictive maintenance and other services to be offered even for brownfield systems. What's more, digitalization enables new business models to be implemented.

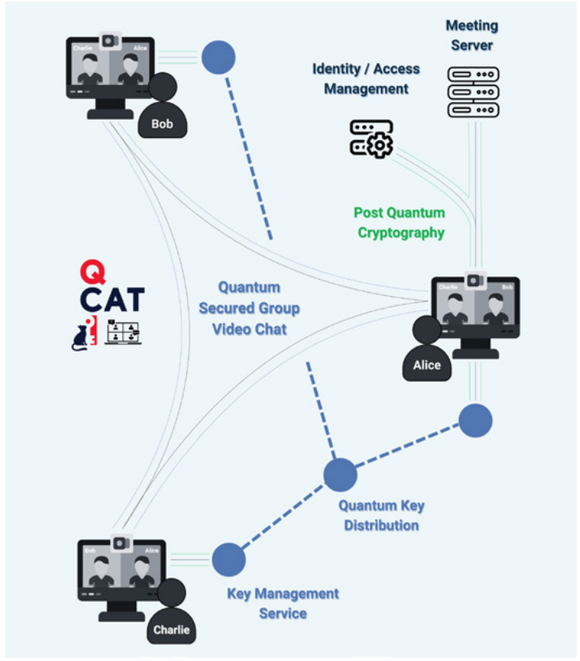
Contact

X-Net Technologies GmbH

Spittelwiese 15, 4020 Linz
Friedolin Baumann
fb@x-net.at

PQC / QKD protected applications

Our goal is to extend open source applications for communication. Beside E2E chat and mail systems, we extend state-of-the art video conferencing systems (e.g. Jitsi, Kurento) with quantum-resistant cryptographic security guarantees. Thereby, both end-to-end authenticity and confidentiality shall be guaranteed by integrating post-quantum secure digital signatures and key exchange algorithms (e.g., via the integration of quantum-resistant TLS). Additionally, for instances of the video conferencing system hosted in data centers with a QKD link, connections are additionally protected by combining the PQC keys with QKD keys from the QKD network. A secure network infrastructure for the key management and the exchange of PQC keys is considered. Our objective is to elaborate findings and technical results as basis for dissemination and creation of later standards and to integrate suggestions for technically feasible methods for post-quantum technology and high-speed networks.



ATLAWS – the Atlas for Tracking Law and Watching Standards – is a digital platform developed under the coordination of the Research Institute to bring clarity and accessibility to the increasingly complex field of European digital legislation. The project responds to a pressing need: making digital legal frameworks more transparent, understandable, and usable for a wide range of stakeholders across sectors.

At the heart of ATLAWS is an open, wiki-based platform that presents EU legal acts in a structured and easily navigable format. Rather than displaying laws in isolation, the platform emphasizes their interconnections, helping users understand how individual regulations relate to one another and to overarching frameworks like the General Data Protection Regulation (GDPR). This approach supports a holistic and interdisciplinary view of the legal landscape and is especially valuable for understanding the regulatory environment in areas such as data spaces, digital sovereignty, and emerging technologies.

ATLAWS is openly accessible under a Creative Commons license and follows an open-source philosophy. By translating abstract legal content into comprehensible language and visual relationships, it makes legal knowledge more approachable—not only for legal professionals, but also for startups, developers, researchers, students, and digital transformation experts. The platform supports early-stage consideration of regulatory requirements, enabling innovation while ensuring legal compliance and fostering quality and trust in digital solutions.

With its flexible and continuously expandable structure, ATLAWS is designed to evolve alongside the legal frameworks it documents. It provides long-term value in a rapidly changing regulatory environment and exemplifies how legal clarity can serve as a foundation for secure and innovative digital development in Europe.

Learn more: https://wiki.atlaws.eu

Mirjam Tercero, Research Institute
Helmut Leopold, AIT
Florian Novotny, BMBWF
Martina Paul, OSSBIG Austria
Ralph Hammer, BMF
David M. Schneeberger, Research Institute
Vincent Bretschneider, AustriaTech

Contact

+43 1 524 3 524 – 0
kontakt@researchinstitute.at
Research Institute

gaia-x Hub Austria

As part of a broader European movement, the Gaia-X Hub Austria facilitates collaboration and knowledge exchange around federated data ecosystems, where data is shared securely and sovereignly. These ecosystems empower organizations to retain full control over their data while benefiting from shared innovation spaces. The hub focuses on practical implementation by connecting existing national activities with European use cases and initiatives.

A key mission of the Gaia-X Hub Austria is to promote the understanding and adoption of data spaces—sector-specific data environments that enable trusted data exchange. Through workshops, stakeholder dialogues, and pilot projects, the hub provides guidance, resources, and strategic input to help Austrian actors navigate the evolving data economy. This includes aligning technical standards, governance models, and business strategies with Gaia-X frameworks.

By fostering transparency, interoperability, and trust, Gaia-X Hub Austria strengthens Austria's position within the European digital landscape. It acts as a bridge between technology and policy, between vision and implementation—supporting a digital future that is open, secure, and aligned with European values.

Learn more: www.gaia-x.at

Contact

Mag. Agnes Jodkowski, BA
agnes.jodkowski@gaia-x.at
Gaia-X Hub Austria

Helmut Leopold
Gerald Steiner
Tobias Höllwarth
Christian Tauber
Stephan Winklbauer
Roland Sommer
Sabine Ringhofer
Annette Trawnicek
Mario Drobics
Georg Hahn

SILKROAD4.0
Driving Growth. Piloting the Future.

XXV.
Global Future Summit

Tech & Diplomacy:
Co-Creating Tomorrow's Relevance Today

November 28, 2025, Worldwide
Organized by SILKROAD 4.0

As the world faces increasing complexity—geopolitical instability, rapid technological disruption, and shifting global alliances—the need for trust-based, cross-sector collaboration has never been more urgent. The Global Future Summit responds to this call.

Following the success of its XXIV edition on May 16th, the XXV. Global Future Summit returns on November 28, 2025, connecting thought leaders, executives, and policymakers across 20+ cities and 8 time zones in a globally synchronized hybrid event. Under the flagship theme Tech & Diplomacy, this initiative by SILKROAD 4.0 blends innovation, international relations, and strategic foresight.

Each summit edition acts as a launchpad for global-impact projects—where stakeholders from business, academia, civil society, and government co-create scalable solutions. With matchmaking formats like the Global Impact Challenge and the Innovation Diplomacy Circles, the summit fosters actionable partnerships at the intersection of sustainability, emerging technologies, and governance.

This is not just a conference.
It's a curated network of networks, actively shaping the future.

Learn more about the Global Future Summit:

www.silkroad40.com/compendium

Contact

Dr. Philipe Reinisch
www.linkedin.com/in/PReinisch

IDSF 2025 – Partners

HOSTED AND ORGANISED BY

AIT Austrian Institute of Technology
WKO Wirtschaftskammer Österreich ARGE Sicherheit & Wirtschaft
KSÖ Kompetenzzentrum Sicheres Österreich

IN COOPERATION WITH

Federal Ministry Republic of Austria European and International Affairs
Federal Chancellery Republic of Austria
Digital Austria
Federal Ministry Finance Republic of Austria
Federal Ministry Interior Republic of Austria
Federal Ministry Defence Republic of Austria
Federal Ministry Innovation, Mobility and Infrastructure Republic of Austria

IN COOPERATION WITH

aed
WKO Wirtschaftskammer Österreich ARGE Sicherheit & Wirtschaft
Digital City .Wien
KIRAS Security Research
VICESSE
Für die Stadt Wien – Kofinanziert von der Europäischen Union
inno·x network
OVE
SILKROAD4.0
European Security and Defence College
VCDNP Vienna Center for Disarmament and Non-Proliferation

LEAD PARTNER

SAAB COMBITECH

WORKSHOP PARTNERS

CMI Martti Ahtisaari Peace Foundation
IAEA
SBA Research
VCDNP Vienna Center for Disarmament and Non-Proliferation
Für die Stadt Wien – Kofinanziert von der Europäischen Union

EXHIBITORS

ABA Invest Work Film – Your easy access to Austria
AIT Austrian Institute of Technology
fragmentiX Quantum Age Cybersecurity
ICSL AT
IKARUS security software
IPDS
IT:U interdisciplinary transformation university austria
The Diplomatic Insight
SBA Research
VCDNP Vienna Center for Disarmament and Non-Proliferation
Für die Stadt Wien – Kofinanziert von der Europäischen Union
X NET

MEDIA

The Diplomatic Insight
Cercle Diplomatique
NEW BUSINESS
Report
IT WELT.at
SICHERHEIT

CONTACT

Please visit the conference website regularly for new information about this conference at idsf.io or send an email to idsf@ait.ac.at for further inquiries.

GREEN EVENT

IDSF25 was again run in accordance with the guidelines for Green Meetings & Green Events.

DESIGN

WHY. Studio

INTERNATIONAL DIGITAL SECURITY FORUM *VIENNA*

www.idsf.io