INTERNATIONAL DIGITAL SECURITY FORUM *VIENNA*

IDSF 2025
Summary Report

Balancing Sovereignty and Solidarity in the Digital Age

IDSF Topic Feature

Technology for peace

AUSTRIAN INSTITUTE OF TECHNOLOGY
WIRTSCHAFTSKAMMER ÖSTERREICH ARGE Sicherheit & Wirtschaft
KSÖ Kompetenzzentrum Sicheres Österreich

Opening

H.E. Zenon Kosiniak Kamysz
Ambassador of the Republic of Poland
to Austria, Poland

H.E. Yvonne Toncic-Sorinj
Deputy Director General for European
and Economic Affairs, Austria

H.E. Nina Vaskunlahti
Ambassador of Finland to Austria and Permanent
Representative to the UN Organizations in Vienna,
Finland

Inhalt

Technology for peace 4

Session 1
Beyond Digital: Tech Diplomacy in a Quantum World 6

Session 2
Bridging Continents: Human-Centric Data Governance and Data Sovereignty for Peace and Security 8

Session 3
The Next Generation of Trusted Data Sharing (Gaia-X) 10

Session 4
Persuasive Technologies: Cognitive Security Risks in the Age of AI, Quantum, and Neurotech 12

Session 5
Responsible R&D by Balancing Innovation and Regulation 14

Session 6
Digital Security & Transnational Infrastructures 16

Session 7
Geopolitics of Cyber Security 18

Session 8
Digital Transformation and the Security Impact on Nuclear Ecosystems and Non-Proliferation 20

Session 9
Building National Resilience through International Cooperation: Cybersecurity Skills Coalition 22

Session 10
From Science and Innovation to Digital Security Ecosystems 24

Session 11
Information Integrity, Disinformation and Societal Impact 26

Session 12
The Fight for Democracy: Censorship vs. Free Speech and Fact-Checking 28

Social Science Track
Digital Sovereignty or Digital Illusion?
Power, Governance, and the Politics of Controlling Big Tech 30

Social Science Track
Democratisation and Policy Recommendations in the Fields of Data Transparency and State Autonomy 32

Social Science Track / Keynote
A New Love for Censorship?
How Social Media and Identity Politics Undermine the Fundamental Values of Democracy 34

Social Science Track
Discussion: Propaganda, Disinformation and Digital Security 36

Workshop
Digital Sovereignty in a Connected World: Navigating Between Openness and Control 38

Workshop
AI for Peace: The Promise and Peril of AI-Powered Engagement in Conflict Zones 40

Workshop
Artificial Intelligence and Cyber Security of High-Risk Critical Infrastructure 42

Impressions IDSF 2025 44

Technology for peace

© AIT/Johannes Zinner

Helmut Leopold
Head of Center for Digital Safety & Security

© Juan Pablo Sierra, Revista Paula

Renata Ávila
CEO of the Open Knowledge Foundation
Practitioner in residence at CIS Sudaco Convention

© AIT/Nathan Coyle

Nathan Coyle
Senior PeaceTech Advisor at the Austrian Institute for Technology

The PeaceTech Alliance, which was first publicly unveiled at the latest International Digital Security Forum (IDSF) in June 2025, brings together partners from research, the public sector and civil society to harness the enormous potential of modern digital technologies for peace-building missions.

Peacekeeping missions around the world also urgently need digital technologies to work effectively on conflict prevention and peacekeeping. However, they often lack the necessary resources at present. Major problems arise, for example, from unreliable digital infrastructures, lack of access to training, failure to involve local peacemakers in the development of suitable tools, and inadequate training data for AI systems, which do not adequately reflect conflicts and their backgrounds.

The non-profit platform 'PeaceTech Alliance', which was presented at the 4th International Digital Security Forum (IDSF) in Vienna in June 2025, aims to be a response to these challenges. It is a human-centred initiative that addresses the responsible design and effective use of modern digital technologies for peacekeeping in a global context. To this end, the platform brings together digital technology experts, social scientists, and representatives of public authorities. We want to support existing activities and bring together various stakeholders so that 1 plus 1 equals 3 instead of 2,' explains Helmut Leopold, initiator of the Peace Tech Alliance and Head of Center for Digital Safety and Security at the AIT Austrian Institute of Technology.

User involvement

The technologies are to be made safer and more sustainable, in particular through co-design approaches: dialogue platforms, joint workshops and the involvement of users in research projects are intended to ensure a better understanding of the development of suitable digital systems and services. In addition, the platform aims to work on recommendations and provide practical assistance via blogs, podcasts and toolkits to support peace activists in continuing their effective work in communities. Responsible technology design is intended to strengthen the human factor in peace operations, while at the same time counteracting undesirable developments at an early stage – for example, by avoiding technical pitfalls such as the ill-considered use of AI systems or inadequate cyber security measures to prevent manipulation and influence.

Broad partnerships

On the initiative of the AIT, organisations from the public sector, science and research, and civil society are involved in the Peace Tech Alliance. Currently, these include the Austrian Centre for Peace, the Diplomatic Academy in Vienna, three universities (University of Innsbruck, University of Graz, Danube University Krems), the Gaia-X Hub Austria, the International Institute for Peace, and the Open Knowledge Foundation. Discussions with other partners are ongoing at Austrian, European and international level.

A central idea is that technology develops and changes through its use and through the setting of framework conditions. 'Every technological development is subject to a permanent shaping process by users and by framework conditions in the form of regulations and laws. Above all, the disruptive changes brought about by digital technology require a new alliance between various stakeholders in order to develop digital solutions that serve our goals and challenges, and thus also to avoid being powerless and at the mercy of technology,' says Leopold.

Collaborative space for developing solutions

In this sense, the PeaceTech Alliance sees itself as a discussion platform and collaborative space for developing skills and modern digital solutions for effective use in conflict prevention and peacebuilding. One major difficulty here is that all norms, standards, etc. are defined for commercial applications. 'To my knowledge, the Peace Tech Alliance is the first initiative that brings together people from the public sector, academia, research, peacebuilding and civil society in Austria to jointly and independently reflect on what PeaceTech actually is – and how we can shape it from the ground up,' explains project manager Nathan Coyle.

He is convinced that Austria is the ideal location for this. 'Austria is neutral and a hot breed for peace organisations. We have the UN, the OSCE and so on here. We want to develop something that is grounded in these communities,' emphasises Coyle. In addition, there is also extensive expertise in the field of security technology in this country, so that in future, peace missions will also be able to draw on local cutting-edge technology for their operations.

Building on existing know-how

The PeaceTech Alliance builds in particular on AIT's high level of expertise in sustainable and responsible digitalisation – including in the areas of cyber security, artificial intelligence (AI) and sovereign data rooms.

The Peace Tech Alliance sees the creation of a trustworthy digital infrastructure and open data spaces as a key challenge. 'In the 20 years that the Open Knowledge Foundation has been active, we have seen that with open technologies and with a high-quality back-bone for key processes, we can enable a lot of collaboration, reduce frictions and activate interoperability, which is crucial for peacebuilding,' explains Renata Ávila, CEO of the Open Knowledge Foundation, which recently joined the Peace Tech Alliance. She adds: 'Of course, we know that technology alone does not create peace, but we also know that the wrong technology choices can trigger conflict. Our contribution to this alliance is therefore to develop technologies, protocols and piloting methodologies that reduce harm, support peace building, strengthen institutions and foster dialogue.' In her view, open standards are essential for people to be able to trust technology.

Trustworthy digital infrastructure

An immediate goal of the Peace Tech Alliance is therefore to build a shared digital infrastructure for peace that all stakeholders can trust and that strengthens communities everywhere. 'A shared decentralised infrastructure is not fighting the commercial platforms, that we already live in, but is complementing a non-commercial part that has not yet been addressed,' says Nathan Coyle.

Digital solutions are to be developed on this basis. 'We are trying to do this in a modular way – our approach is to listen to communities to find out what they really need. The technologies should be adaptable and able to be redesigned to meet the needs of specific communities.' As examples of peace-building tools, he cited an app that people in Kenya can use to document atrocities and then use those as a medium to hold people accountable, and a satellite-based system that is used in South Sudan to track down missing cattle, which often leads to serious conflicts, to say what really happened.

'Particularly in sensitive areas such as peace work, where confidential information is exchanged across borders, there is a need for cooperative, trust-based dialogue on the design of technological solutions,' emphasises Helmut Leopold. The AIT is working with many partners within the framework of the European Gaia-X initiative on mechanisms for sovereign and trustworthy data exchange between different actors. Gaia-X is a significant contribution to sustainable data sovereignty in Europe. A key question here is how trustworthy data can flow efficiently and how a trustrd framework can be implemented in such a way that the mechanisms for data verification are handled autonomously between computers – and not by human beings because that's not scalable. 'This Gaia-X Trust Framework is also to be transferred to PeaceTech in order to achieve trust, interoperability and security for the necessary exchange of data between public authorities and private organisations in a global context in a very sensitive area,' explains Leopold.

Award-winning initiative

Although the Peace Tech Alliance is still very young, it has already attracted considerable public interest and has been awarded one of the most important prizes for Austria's digital community, namely the eAward in the 'Sustainability' category.

A key objective of the Peace Tech Alliance is to ensure the effective, but above all ethical and responsible use of modern digital technology for conflict prevention and peacekeeping.

Session 1

Beyond Digital: Tech Diplomacy in a Quantum World

Chair

Claudia Reinprecht
Head of Department for Telecommunications, Digital and Tech Diplomacy, Austrian Ministry for European and International Affairs, Austria

Panelists

Ditte Bjerregaard
Acting Tech Ambassador, Ministry of Foreign Affairs of Denmark

Ulrich Mans
Lead Strategic Partnerships, Quantum Delta, Netherlands

Zeki Seskir
Doctoral Researcher at Institute for Technology Assessment and Systems Analysis (KIT-ITAS), Germany

Michal Krelina
Associate Senior Researcher, SIPRI – Stockholm International Peace Research Institute, Sweden

Quantum technologies, while still at an early stage of development, are expected to challenge existing security paradigms in fundamental ways. The session framed the discussion around the potential impact of quantum on secure communications, critical infrastructure, and broader peace and security agendas. Emerging quantum capabilities were discussed in relation to their possible effects on military operations, defence strategies, and strategic stability, as well as on weapons development, arms control, non-proliferation, and economic security. Particular attention was given to questions of technology sovereignty and export controls. Against this backdrop, the session examined how quantum technologies intersect with digital sovereignty, cybersecurity, and global security architectures, and how diplomatic engagement can help shape norms, cooperation mechanisms, and governance frameworks in order to prevent fragmentation and support a secure and balanced technological future.

The discussion addressed the strategic and diplomatic dimensions of quantum technologies, emphasising their growing geopolitical relevance and their potential to reshape international relations. The importance of sustained diplomatic engagement was highlighted in guiding debates around the EU Quantum Strategy, the forthcoming Quantum Act, and the proposed Quantum Pact, with a view to ensuring a strong role for the EU's Common Foreign and Security Policy and Common Security and Defence Policy. The session also explored EU–NATO cooperation in the quantum domain and considered how non-NATO EU member states could be meaningfully involved. The urgency of global competition in quantum was underlined, alongside the need for ambitious, partnership-driven approaches to strengthen Europe's position.

Geopolitical dynamics surrounding quantum innovation and cooperation were further analysed, with the EU described as facing a strategic crossroads. Growing international competition was seen as reshaping patterns of collaboration and scientific progress, marking a shift from default globalism toward more selective bilateral arrangements. This shift was linked to emerging economic security challenges, including export controls and research protection measures. The discussion stressed the need for clearer diplomatic structures and narratives around quantum technologies, as well as the importance of demonstrating trustworthiness and ethical awareness in international engagement. The absence of a traditional marketplace for quantum technologies was identified as an opportunity to design new regulatory and governance approaches tailored specifically to quantum, rather than adapting existing frameworks developed for semiconductors or other technologies. Attention was also drawn to dual-use considerations, NATO's evolving strategic posture, and initiatives such as "ReArm Europe", highlighting the need to align European innovation with broader security objectives.

Responsible quantum innovation emerged as a central theme, with calls for a holistic approach that integrates ethical, legal, and design considerations from the outset. Societal readiness was identified as a critical challenge, requiring significant shifts in public understanding and acceptance of quantum security technologies. The risk of social backlash and public alienation was noted, underscoring the importance of proactive public engagement. In this context, the concept of an "ELSA for Quantum" framework was discussed, focusing on the ethical, legal, and social aspects of quantum technologies. While such frameworks are increasingly well developed in theory, practical implementation was seen as lagging behind. The session therefore highlighted the need for targeted capacity-building initiatives across the EU to ensure that both institutions and the workforce are prepared for the emerging quantum landscape.

The military and security implications of quantum technologies were also examined, particularly their potential influence on strategic stability, deterrence, and the risk of a future quantum arms race. The discussion stressed the importance of proactive international risk management to prevent escalation or misuse, alongside the identification of vulnerabilities in critical infrastructure.

Overall, the session underscored that quantum technologies represent not only a technical challenge but also a societal and strategic one. Ethical awareness, public engagement, international cooperation, and regulatory foresight were repeatedly highlighted as essential elements. The discussion concluded by emphasising the role of tech diplomacy in developing governance frameworks that safeguard democratic values while protecting strategic and technological interests, and by reaffirming the importance of sustained dialogue between technology, policy, and diplomacy in navigating the quantum era.

Session 2

Bridging Continents: Human-Centric Data Governance and Data Sovereignty for Peace and Security

Chair

Nathan Coyle
Senior PeaceTech Advisor AIT Austrian Institute of Technology, Austria

Panelists

Renata Ávila Pinto
CEO of Open Knowledge Foundation, United Kingdom

Markus Kornprobst
Vienna School of International Studies, Diplomatische Akademie Wien, Professor of International Relations, Austria

Farhat Asif
Founder & President, Institute of Peace & Diplomatic Studies, Islamabad, Pakistan

Tobias Lang
Director, Austrian Centre for Peace, Austria

At IDSF 2025, the PeaceTech Alliance was launched as a nationwide platform dedicated to peacebuilder-first design. Housed at the AIT Austrian Institute of Technology and developed in partnership with Gaia-X Austria, the Austrian Centre for Peace, the International Institute for Peace, the University of Innsbruck, the University of Graz, the Diplomatic Academy of Vienna, Danube University Krems, and the Open Knowledge Foundation, the Alliance was presented as a collaborative hub for research, innovation, and practice. Its establishment reflects an ambition to position Austria as a leading location for human-centric PeaceTech.

The session addressed a fundamental question: whether the data and tools currently used in peacebuilding are truly fit for purpose. The discussion emphasised that PeaceTech must be designed with and for those who use it in practice. Without collaborative design processes, technology risks becoming irrelevant. Particular attention was given to the need for narratives that resonate with peacebuilders on the ground, moving beyond technical jargon and focusing on the concrete ways digital tools can support community development and conflict resolution.

A central theme was the importance of perspectives from the Global South. As the role of artificial intelligence in peacebuilding continues to expand, the discussion highlighted the structural biases embedded in the data that underpin these systems. While the majority of conflicts take place outside Europe and North America, more than 90% of AI training datasets originate from these regions. Western-centric datasets and governance models were therefore seen as insufficient to reflect local realities. The session underlined the need for partnerships that embed legitimacy and inclusivity, as well as for recognition of traditional conflict resolution practices that are often absent from digital tools. Grounding innovation in local knowledge was considered essential to ensuring that PeaceTech meaningfully supports peace and security efforts.

The discussion further explored the role of data commons as ethical and participatory environments in which communities can shape and own the data that affects them. Data sovereignty was framed not as an abstract technical goal, but as a practical requirement for effective peacebuilding. Transparency, control, and trust were identified as preconditions for the meaningful use of digital tools. If technologies are not understandable and accessible in local contexts, they risk being ineffective or potentially harmful.

The session concluded with a clear call to action. PeaceTech should be co-designed with peacebuilders and local communities, embedding data sovereignty, accessibility, and trust at its core. Only through such approaches can digital tools and datasets become genuinely fit for purpose and empower those most affected by conflict. The launch of the PeaceTech Alliance at IDSF 2025 was presented as a concrete commitment to advancing this vision by connecting research, practitioners, and communities to co-create human-centric PeaceTech and translate these principles into practice.

Session 3

The Next Generation of Trusted Data Sharing (Gaia-X)

Chair

Roland Fadrany
Chief Operating Officer,
Gaia-X AISBL, EU

Panelists

Detlef Eckert
Founder Deep Digital Consulting B.V.,
Author of “40 Years of European
Digital Policies“, Belgium

Senadin Alisic
Strategy Advisor, Combitech AB,
Sweden

Insuk Kim
President of Korean-German Association of
Economics and Management (KDGW),
CEO of HANDA Forum, South Korea

The session explored the premise that sovereign digital ecosystems, or data spaces, form the foundation of a competitive economy and a self-determined digital future. Against current market developments, the discussion highlighted the risk of declining value creation, prosperity, and sovereignty for individual states and companies if such ecosystems are not established. Data was consistently framed as the core resource of digital ecosystems and a prerequisite for any effective AI strategy. In this context, the session examined how data space initiatives such as Gaia-X are driving transformation by enabling trusted and secure data sharing.

The discussion was structured around three introductory presentations followed by a roundtable exchange. These inputs addressed the strategic potential of data strategies, the role of Gaia-X in enabling sovereign and interoperable data spaces, and experiences with Gaia-X compliance beyond Europe. Together, they set the basis for a broader debate on adapting data strategy and governance as integral elements of digital transformation in the corporate sector, on building decentralized and interoperable data space ecosystems based on the Gaia-X Trust Framework, and on the international dissemination of Gaia-X as part of strategic cooperation between the EU and the Republic of Korea. The subsequent discussion also reflected on the role of the EU in balancing data protection and regulation.

From an industry perspective, it was noted that the shift toward interconnected ecosystems and collaboration-oriented data spaces has been underway for decades, particularly in industrial high-tech sectors with complex, multi-tier supply chains. The example of aerospace manufacturing illustrated the scale of coordination required, where millions of components from thousands of suppliers must be validated against stringent safety standards through secure data exchange. Such environments depend on highly secure and reliable data channels.

Within this ecosystem economy, several persistent challenges for companies developing long-term data strategies were identified. These include the absence of coherent data strategies, fragmented data across legacy systems, inconsistent data quality and access conditions, insufficient analytical and infrastructural capabilities, and difficulties in monetising data and data-driven services. A distinction was drawn between intra-data strategies, focused on internal operational excellence and compliance, and inter-data strategies, which enable deeper customer understanding, improved products and services, and the creation of new revenue streams within data ecosystems.

The rise of decentralized, many-to-many data ecosystems has significantly increased demand for standardized data spaces. Gaia-X was presented as a trust framework designed to meet this demand, based on jointly defined architectures and standards agreed by its members. Gaia-X–based data spaces establish their own onboarding processes, governance authorities, and applicable rules. By analogy, this governance approach was compared to international travel systems, where shared legal requirements coexist with nationally defined processes and authorities.

The evolution from centralized data platforms toward federated data ecosystems was described as a key development. In the Gaia-X ecosystem, participants and services are verified by Gaia-X Digital Clearing Houses in terms of trust, sovereignty, and interoperability. This federated approach avoids single points of failure and was characterised as a form of democratised trust. Examples of existing Gaia-X–compliant ecosystems were referenced across sectors such as automotive, aerospace, energy, smart cities, and supplier networks, all facing significant regulatory and transformation pressures.

The Gaia-X Trust Framework was outlined as a governance model covering design, build, and run phases. Different requirements apply to the Gaia-X community, the open-source software community, and service providers acting as Gaia-X Digital Clearing Houses. At the time of discussion, twelve such clearing houses were already operational. Overall, the framework was described as meeting core trust requirements between participants, enabling access to high-quality data, fostering interoperable ecosystems, and responding to the complexity of global legislation.

International cooperation formed a significant part of the discussion. Ongoing collaboration between Germany and South Korea on Gaia-X compliance was highlighted, with a focus on legislative and organisational interoperability and the exploration of governance models for global data communities. Future efforts aim to establish bilateral data space business communities in areas such as agriculture, smart health, energy, and manufacturing, with particular attention to the circular economy across the data service lifecycle. Consideration of Korean data legislation, including personal data protection and sector-specific promotion acts, was also discussed in relation to Gaia-X connection points.

Further internationalisation examples included cooperation with Canada, where differing national digital identity systems pose trust challenges, and a project in the Caribbean, where interconnected data centres opted for Gaia-X compliance to ensure comparability and service mobility across islands. These cases illustrated how Gaia-X compliance can support interoperability and resilience in diverse regulatory and geographic contexts.

From a digital policy perspective, two approaches were highlighted to strengthen the market position of European companies in cybersecurity and digital sovereignty. The first emphasised the role of a key stakeholder as custodian of data ecosystems to scale adoption, with the Catena-X lighthouse project cited as a reference model. The second addressed regulatory complexity, noting ongoing efforts in Brussels to simplify rules through omnibus regulation.

The session concluded with a shared view that early public procurement of innovative solutions from start-ups and SMEs is essential for building digital sovereignty and international industrial capability, and should be considered a core element of strategic policy toolkits.

Session 4

Persuasive Technologies: Cognitive Security Risks in the Age of AI, Quantum, and Neurotech

The session examined the dual-use nature of emerging technologies and their growing implications for mental integrity and privacy. The discussion was framed around the question of whether existing legal and regulatory systems are equipped to address the risks posed by advances in artificial intelligence, neurotechnology, and quantum-enabled tools. Particular attention was given to the tension between rapid technological innovation and the protection of individual cognitive security.

Chair

Claudia Reinprecht
Head of Department for Telecommunications, Digital and Tech Diplomacy, Austrian Ministry for European and International Affairs, Austria

Panelists

Guilherme Maia de Oliveira Wood
Head of the Section for Neuropsychology and Neuroimaging, Karl-Franzens-Universität Graz, Austria

Jean-Marc Rickli
Head of Global and Emerging Risks, Geneva Centre for Security Policy, Switzerland

Alexandra Duca
Legal Advisor, Federal Ministry of Defence, Austria

Wenzel Mehnert
Futurologist at the AIT Austrian Institute of Technology, Austria

The manipulative potential of neurodata and brain–computer interfaces was highlighted, including risks that extend beyond direct health impacts, even in cases of voluntary use. While current neurotechnologies remain limited in precision, they were described as already capable of influencing human behaviour. The discussion raised concerns about how public and societal narratives around neurotechnology may evolve in ways that enable subversion or misuse. Legal ambiguities were also addressed, especially regarding the applicability of existing frameworks governing war and peace to hybrid forms of cognitive conflict.

Cognitive warfare was explored in the context of contemporary conflicts, where AI is increasingly used for data analysis, pattern recognition, and targeting support. The expanding role of AI-enabled drones, including autonomous navigation and the prospective deployment of drone swarms, was discussed as an illustration of shifting cost and capability dynamics in warfare. Cyber and digital operations were described as increasingly inseparable from physical conflict, with AI enabling autonomous malware, tailored disinformation, and large-scale cognitive manipulation. These developments were seen as contributing to changes in global power balances and increasing Europe's vulnerability due to its reliance on external technologies and platforms. Information control and cognitive influence were therefore identified as central elements of modern conflict, reinforcing the need for resilience, regulatory foresight, and proactive policy responses.

The legal dimensions of emerging cognitive technologies were further examined, with existing international instruments described as often too broad or outdated to address current and future risks. Psychological operations that incite violence were noted as already prohibited under international law, and the argument was advanced that mental integrity should be afforded protections comparable to physical integrity within the law of armed conflict. Rather than relying exclusively on new legislation, the discussion emphasised the value of flexible legal approaches, including soft law mechanisms, reflecting the dynamic and interpretative nature of international law.

The complexity of applying legal norms across war and peace contexts was also highlighted, including situations in which self-defence may involve kinetic responses.

A strategic foresight perspective addressed the role of hype and fear in accelerating the adoption of emerging technologies. High-profile examples were cited to illustrate how innovation often advances more rapidly than the development of regulation and norms, creating tensions with existing legal frameworks, including those related to intellectual property. Social media was described as an established battleground for influencing thought and behaviour, reinforcing the view that technological fixes alone are insufficient and that broader societal and policy responses are required to address cognitive security risks.

The discussion concluded with reflections on accountability and enforcement. Challenges in holding companies responsible for the societal impacts of their technologies were noted, alongside the difficulty of enforcing international law in cases of disinformation and cognitive manipulation. The role of technology companies as political actors, for example through content moderation decisions, was also highlighted. Overall, the session underscored the need for heightened awareness of the risks associated with neurotechnology and persuasive technologies, and for aligning innovation with protective norms that safeguard cognitive integrity.

Session 5

Responsible R&D by Balancing Innovation and Regulation

Chair

Christof Tschohl
Research Director, Research Institute, Austria

Panelists

Sebastian Kneidinger
Policy Advisor, epicenter.works, Austria

Orion Forowycz
CTO Nexus Group AI, Austria

Sarah Kriesche
Journalist (ORF Radio – Ö1/FM4), Austria

Madeleine Müller
Senior Researcher at Research Institute – Digital Human Rights Center, Austria

Introducing ATLAWS (Atlas for Tracking Law And Watching Standards), the session focused on how technological development in the digital domain can be advanced without neglecting regulatory requirements. The discussion addressed the challenge of promoting innovation while ensuring compliance within an increasingly complex European regulatory landscape, particularly in areas related to cybersecurity and digitalisation.

A central issue was the growing complexity and accessibility of regulation. Reference was made to the rapid expansion of EU digital legislation in recent years, including instruments such as the AI Act, the Data Act, NIS2, and the Cyber Resilience Act. This proliferation of legal acts was discussed as a significant challenge for organisations seeking to maintain legal certainty while keeping pace with fast-moving technological developments. Against this background, the session explored how regulatory clarity and innovation can be reconciled in practice rather than perceived as competing objectives.

ATLAWS (https://wiki.atlaws.eu) was presented as a concrete response to these challenges. The digital platform is designed to provide structured, reliable guidance through EU digital legislation and its links to national legal frameworks. Its wiki-based, intuitive format was discussed as a means to reduce legal complexity in a meaningful way and to make regulatory requirements more accessible not only to legal experts, but also to developers, researchers, and organisations active in the digital economy.

The discussion highlighted key characteristics of the platform, including its division into four thematic clusters, the use of practical application examples, and its interdisciplinary and collaborative approach. These elements were presented as mechanisms to support compliance-oriented innovation and to ease the regulatory burden across the Austrian and European digital economy. The platform was described as the result of close collaboration between research and industry, with ongoing efforts focused on building a sustainable and active community around the ATLAWS initiative.

More broadly, the session underlined that legal certainty and innovation are not mutually exclusive. Through dialogue and practical tools such as ATLAWS, regulatory frameworks can provide orientation, trust, and guidance while still enabling responsible research and development. Making regulation understandable and usable in practice was seen as a prerequisite for fostering innovation that aligns with fundamental rights and policy objectives.

The session concluded by emphasising the importance of continued exchange between policymakers, researchers, industry, and media in shaping a digital and legal environment that supports both innovation and regulation. The discussion was positioned as a constructive contribution to the ongoing development of Austria's and Europe's digital regulatory landscape.

Session 6

Digital Security & Transnational Infrastructures

Chair

Eric Eifert
Cyber Security Research Engineer,
AIT Austrian Institute of Technology, Austria

Panelists

Georgios Kolliarakis
Coordinator EU P2P Global Dual-Use Programme, Foreign Policy Instrument/ European External Action Service (EEAS), EU

Eman Al Awadhi
Vice President Network and Cyber Security, Expo City Dubai, United Arab Emirates

Salmi Ahsan
Security Solution Advisor, SAP Berlin, Germany

José Carrera
International Governance, Risk & Compliance (GRC) Thought Leader and Cybersecurity Strategist, United Arab Emirates

The session examined the challenges organisations face when operating global digital infrastructures that rely on software and infrastructure delivered as a service. Complex transnational operating models were discussed, in which incidents can involve victims, infrastructure, workforces, and potential attackers located across multiple jurisdictions. Against this background, the discussion highlighted the growing relevance of data sovereignty and the need for clear guidance and legal frameworks that reflect these realities. Drawing on perspectives ranging from smart city development to global SaaS operations, the session explored how security, governance, and regulation must evolve to support globally distributed infrastructures.

A practical illustration focused on how Expo 2020 Dubai established the foundations for a future-ready smart city through the strategic design and deployment of digital infrastructure. The discussion emphasised long-term adaptability as a core design principle, enabling temporary event infrastructure to be transformed into a permanent, multi-purpose digital platform for Expo City and future large-scale international events. This approach demonstrated how early architectural decisions can support sustainability, scalability, and long-term value creation.

Particular attention was given to the early adoption of software-defined network architectures. This model was discussed as a key enabler of agility, centralised management, and enhanced cybersecurity. By allowing infrastructure components to be reused efficiently, the approach illustrated how targeted digital investments can strengthen operational resilience while also delivering measurable cost efficiencies.

The role of digital sovereignty in an increasingly interconnected environment formed another central theme. The discussion highlighted hybrid cloud models, strong governance structures, and embedded security as mechanisms to maintain national or organisational control while still benefiting from global technology platforms. Expo City was referenced as an example of how large-scale initiatives can balance innovation, scalability, and sovereignty within a coherent digital strategy.

The session then broadened the perspective to governance, risk, and compliance (GRC) as critical enablers of sovereignty and infrastructure resilience. National digital infrastructure was framed as a strategic asset, with an emphasis on the need for states to retain control over data, cloud services, and AI platforms without constraining innovation. Embedding sovereignty considerations into digital transformation strategies was seen as essential. Effective GRC frameworks were discussed as a means to secure digital ecosystems, with key elements including clear ownership and accountability, transnational risk mitigation, and regulatory compliance. Existing regulatory and governance models were referenced as practical examples of how robust GRC can support both innovation and resilience.

Cross-border collaboration was identified as a necessary complement to national control. The discussion underscored that digital resilience increasingly depends on shared threat intelligence, regulatory harmonisation, and joint exercises. Strategic alliances and cooperative mechanisms were presented as ways to enhance collective resilience while preserving sovereignty. At the same time, the growing dependence on global cloud and AI providers was recognised as introducing new risk dimensions, requiring careful balancing of innovation, data localisation, legal jurisdiction, and ethical governance through approaches such as sovereign cloud solutions.

The session concluded by outlining strategic considerations for governments, including investment in national and regional infrastructure, the strengthening of regulatory and GRC capabilities, and the promotion of public–private partnerships. Security and resilience were ultimately framed not as constraints, but as growth enablers that underpin economic stability and trust. The discussion reinforced the view that national security and economic progress are increasingly interlinked in the digital age.

Session 7

Geopolitics of Cyber Security

Chair

Karin Kosina
Head of Cyber Diplomacy Unit, Federal Ministry for European and International Affairs, Austria

Participants

Joanna Pawełek-Mendez
Coordinator for Cybersecurity Policy, Ministry of Foreign Affairs, Poland

Szilvia Tóth
Cyber Security Officer, OSCE Secretariat, Transnational Threats Department, Austria

Olesia Mariina
Member of the Security Service of Ukraine, Ukraine

The session examined the geopolitical and security policy dimensions of malicious cyber activities and the range of policy responses developed by states to prevent, deter, and respond to these threats. The discussion focused on how cyber operations by both state and non-state actors increasingly affect national security, democratic institutions, and critical infrastructure, and how these developments challenge existing international norms and policy frameworks.

Malicious cyber activities were described as an escalating threat to both national and European security. Attacks targeting critical infrastructure and democratic processes were discussed as being incompatible with international law and with the norms of responsible state behaviour in cyberspace endorsed by all UN Member States. Against this backdrop, the session highlighted the growing relevance of cyber diplomacy as an integral element of foreign and security policy.

The discussion outlined the EU's policy response to malicious cyber activities, with particular attention given to the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, commonly referred to as the Cyber Diplomacy Toolbox. Established in 2017, the framework enables the EU and its Member States to draw on the full range of instruments available under the Common Foreign and Security Policy, including restrictive measures where necessary. The use of public statements condemning malicious cyber behaviour and calling for responsible conduct in cyberspace was highlighted as one of the most visible applications of the toolbox. In addition, the framework encompasses diplomatic engagement, cooperation and coordination within the EU and with international partners, as well as capacity-building measures. The cyber sanctions regime introduced in 2019 was discussed as a further component, applying to significant cyber attacks originating outside the EU and currently targeting a defined number of individuals and entities.

The role of international organisations in reducing cyber-related risks was also addressed. The discussion examined how established arms control experience has been adapted to the digital domain through confidence-building measures designed to lower the risk of conflict arising from the use of information and communication technologies. A set of confidence-building measures adopted since 2013 was highlighted, combining transparency measures aimed at strengthening cyber resilience and preparedness with cooperative measures focused on communication channels, public–private partnerships, critical infrastructure protection, and information sharing on vulnerabilities.

During the subsequent exchange, further issues were explored, including the application of international law to cyber activities, the role of cyber operations within the broader hybrid threat landscape, and the persistent challenges associated with attribution. The increasing blurring of boundaries between cybercrime, hacktivism, state-sponsored cyber operations, and cyber activities conducted in the context of military conflicts was identified as a particular concern for policymakers and practitioners alike.

The session concluded with the observation that malicious cyber activities are likely to continue increasing in frequency, scale, and sophistication. Preventing, deterring, and responding to these threats will therefore require the consistent and coordinated use of all available political, diplomatic, and regulatory instruments. As cyberspace is increasingly used as a domain of geopolitical confrontation, cyber security was framed not as a purely technical issue, but as a core component of national security and state resilience.

Digital Transformation and the Security Impact on Nuclear Ecosystems and Non-Proliferation

Chair

Donald Dudenhoeffer
Cyber Security Research Engineer, Security & Communication Technologies, AIT Austrian Institute of Techology, Austria

Panelists

Sarah Case Lackner
Senior Fellow, Vienna Center for Disarmament and Non-Proliferation (VCDNP), Austria

Lars von Dassen
Executive Director World Institute for Nuclear Security (WINS), Austria

Paul Smith
Professor, Chair in Networking, Lancaster University, United Kingdom

Ulrik P. Ahnfeldt-Mollerup
Head of Section at UN Office of Counter-Terrorism, UNOCT

Rodney Busquim
Head of the Information Management Section, Division of Nuclear Security, Department of Nuclear, Safety and Security, International Atomic Energy Agency (IAEA)

The session examined the accelerating digital transformation across society and industry and its implications for security, resilience, and governance in the nuclear domain. Driven by the convergence of advanced technologies, digitalisation offers significant opportunities, while also introducing complex challenges. Technologically induced workforce disruption, adversarial uses of emerging tools, and regulatory frameworks struggling to keep pace with rapid innovation were highlighted as key elements shaping the current landscape.

As a cornerstone of the global energy system, the nuclear sector is increasingly dependent on advanced digital technologies such as artificial intelligence, cloud computing, and automation. These technologies were discussed as essential for maintaining and optimising existing nuclear facilities, as well as for the design and deployment of next-generation reactors in response to rising energy demands. At the same time, digital innovation was framed as a critical component of nuclear security, supporting the protection of nuclear materials and sensitive information and contributing to global non-proliferation efforts and the prevention of terrorist access.

The discussion brought together multidisciplinary perspectives to examine how digital transformation is reshaping nuclear safeguards and security. The session explored how technology can be leveraged to strengthen the resilience of nuclear ecosystems, while also addressing emerging risks, including the malicious use of AI and other advanced tools.

From a non-governmental perspective, the discussion addressed both nuclear security and non-proliferation dimensions. Nuclear security challenges were examined alongside initiatives aimed at increasing awareness and understanding of non-proliferation issues within the industry, particularly through education and training. These contributions underscored the importance of building institutional and human capacity alongside technological advancement.

The role of AI in counter-terrorism and global nuclear governance was also discussed. AI-enabled tools were examined in the context of efforts to counter terrorism, as well as initiatives designed to support states in understanding and managing the applications and implications of AI within the nuclear sector. Attention was given to the need for guidance and support structures that enable responsible and secure adoption of these technologies.

Regulatory and governance considerations formed another key strand of the discussion. Emerging approaches to regulating AI deployment in critical industries were explored, highlighting the need for governance models that can address both innovation and risk in highly sensitive sectors such as nuclear energy.

Across the discussion, a unifying message emerged: AI and other advanced digital technologies are set to play an expanding role in critical infrastructures, including nuclear ecosystems. While their potential benefits are considerable, the associated risks require careful management. Limited practical experience among operators in deploying AI for security and industrial purposes was identified as a particular challenge. As digital capabilities evolve, continued education, outreach, and knowledge-sharing were emphasised as essential to support policymakers, practitioners, and technical stakeholders in navigating the security and non-proliferation implications of digital transformation.

Session 9

Building National Resilience through International Cooperation: Cybersecurity Skills Coalition

Chair

Christian Rupp
former Federal Executive Secretary eGov Austria and Board Member of the Nationale eGovernment Competence Centre in Berlin, Austria

Panelists

Vangelis Ouzounis
Head of Capacity Building and Skills Unit, ENISA, EU

Michail Bletsas
Governor of the NCSA (National Cyber Security Authority), Greece

Uroš Svete
Director of the Government Information Security Office of the Republic of Slovenia, Slovenia

Aleksandra Mudrinić Ribić
Deputy CEO Education Support Department in CARNET (Croatian Academic and Research Network), Croatia

Natalia Spinu
Director of the European Institute for Political Studies in Moldova, Moldova

Blerim Rexha
Professor at the University of Prishtina, Faculty of Electrical and Computer Engineering in Prishtina, Kosovo

The session examined how national resilience in the face of escalating cyber threats depends on effective and coordinated capacity building. The discussion focused on the role of targeted training and education programmes in strengthening preparedness, as well as on the importance of international cooperation in addressing persistent cybersecurity skills gaps.

National resilience in cybersecurity was discussed as being closely linked to cross-border collaboration, particularly for smaller countries such as Moldova. Key challenges identified included the duplication of efforts among national structures such as Computer Emergency Response Teams (CERTs) and training academies, curricula that are insufficiently aligned with practical needs, and a lack of qualified instructors. Beyond attracting young people to the field, retaining skilled professionals over time was highlighted as a critical issue for sustainable capacity building.

European-level efforts to structure and professionalise cybersecurity skills development formed another focus of the discussion. The role of ENISA, the EU Agency for Cybersecurity, was highlighted in this context, particularly its long-standing engagement in cyber capacity building and skills development. The European Cyber Skills Framework (ECSF) was referenced as a widely adopted instrument that provides a common reference across EU Member States. At the same time, persistent fragmentation at national level was identified as a major obstacle to achieving coherence and comparability across Europe.

Cybersecurity was consistently framed as a transnational challenge that cannot be addressed through purely national approaches. Strengthening resilience was linked to international and bilateral cooperation, as well as to the concept of digital solidarity. This was described as including not only openness to cooperation, but also the willingness to share experiences, including negative incidents and lessons learned, in order to support collective prevention and preparedness.

The contribution of academia and educational institutions was emphasised as a key pillar of long-term resilience. Universities were discussed as playing a central role in educating a new generation of cybersecurity professionals capable of protecting the digital environment. In parallel, the importance of broader awareness-raising beyond expert communities was highlighted. National research and education networks such as CARNET (Croatian Academic and Research Network) were referenced as examples of organisations that act as hubs for developing educational materials and promoting cybersecurity awareness across society.

The session also addressed emerging European initiatives aimed at closing the cybersecurity skills gap through structured cooperation. In this context, the establishment of a Cyber Skills Academy in Athens under a European Digital Infrastructure Consortium (EDIC), involving Greece alongside Croatia, Slovenia, Austria, and Cyprus, was discussed. The initiative aims to coordinate and strengthen existing training, upskilling, and reskilling programmes for cybersecurity professionals across Europe.

The discussion concluded by reaffirming that enhanced cooperation in cybersecurity skills training and education is a central element in adapting societies to emerging digital threats. Sustained commitment to international collaboration, capacity building, and shared responsibility was identified as essential for strengthening national and European cybersecurity resilience.

Session 10

From Science and Innovation to Digital Security Ecosystems

Chair

Helmut Leopold
Initiator IDSF, Head of Center for Digital Safety & Security at AIT Austrian Institute of Technology, Vice-President Competence Center Secure Austria (KSÖ), Austria

Panelists

Ralph Hammer
Director of the Staff Department for Security Research and Technology Transfer at the Austrian Federal Ministry for Finance (BMF), Austria

Jeannette Klonk
Programme Manager, National Contact Point for Civil Security for Society, Austrian Research Promotion Agency (FFG), Austria

Birgit Reiter-Braunwieser
Team Lead Research Location & CEE: Cyber security company landscape in Austria and ABA support for international companies, Austria

Hubert Cottogni
Director, European Investment Bank, Austria

The session explored how scientific research and technological innovation can be translated more effectively into real-world applications within digital security ecosystems, against the backdrop of digital sovereignty and growing geopolitical pressure. The discussion focused on how targeted funding instruments at national and European level can help bridge the gap between research, market adoption, and societal needs.

A central premise was that digital transformation generates not only technological opportunities but also challenges for market uptake and public acceptance, particularly in the security domain. Innovation was therefore framed as a process that must be embedded in dialogue, awareness building, and continuous exchange among stakeholders. The session provided an overview of how Austria's innovation and funding ecosystem is designed to support responsible and impact-oriented security research along the entire value chain.

Austria's long-standing role as a frontrunner in security research funding was highlighted, particularly through programmes such as KIRAS for civil security research (https://www.kiras.at) and FORTE in the defence domain (https://www.forte-bmf.at). A defining characteristic of these programmes is the mandatory involvement of broad consortia, bringing together practitioners and end-users, researchers, Austrian companies, and experts from the social sciences and humanities to ensure relevance, usability, and public acceptance. Over time, these instruments have been integrated into the Austria Safety PIN (Sicherheits-Klammer) framework (https://www.k-pass.at), combining civil and defence research and enabling outcomes at Technology Readiness Levels (TRL) 4–6.

Recent efforts to further strengthen this ecosystem were discussed, including the linkage of the Cybernet Pass (K-Pass) research programme with the established Austria Safety PIN framework. This approach aims to support Austrian companies in generating market-near research results and overcoming the "valley of death" between research and commercialization. Increased internationalisation was also identified as a strategic objective, with a growing share of projects open to non-Austrian entities.

At European level, the discussion focused on Horizon Europe (https://www.ffg.at/en/Europe/HorizonEurope), in particular Cluster 3 on Civil Security for Society and applied cyber security research. Similarities with national programmes such as KIRAS were noted, including the requirement to involve practitioners in project consortia. Key thematic priorities include fighting crime and terrorism, border management, resilient infrastructures, disaster resilience, and cyber security. In addition to technological development, Horizon Europe places strong emphasis on societal aspects and engagement with civil actors. Differences between funding instruments across basic research, applied research, and deployment phases were also highlighted, alongside efforts to improve European competitiveness while safeguarding autonomy and supply chains.

Austria's positioning as a business- and innovation-friendly location for digital security was further discussed. The Austrian Business Agency (ABA) was presented as a central support structure, providing access to national and European funding landscapes, overviews of the Austrian cyber security ecosystem, and information on venture capital and education opportunities (https://aba.gv.at) . These services are offered free of charge as part of Austria's strategy to attract international cyber security companies and R&D start-ups.

Finally, the role of financing and investment was addressed through the perspective of the European Investment Bank (EIB). The EIB was described as a key actor in supporting the scaling and growth of European cyber security companies, with security and defence framed as transversal priorities linked to digitalisation and innovation. Europe's competitiveness was linked to increased investment, a unified Capital Markets Union, closer cooperation between public and private investors, and investor-friendly regulation.

The session concluded with the shared understanding that Austria and Europe possess substantial "brain capital" in digital security. Translating this potential into resilient digital security ecosystems requires coherent funding strategies, strong cooperation across the innovation chain, sufficient investment, and greater confidence in Europe's own capabilities.

Session 11

Augusto Lopez Claros
Executive Director, Global Governance Forum, Spain

Opening Speech and Session 11 on Day 3

Information Integrity, Disinformation and Societal Impact

Chair

Ross King
Head of the Competence Unit Data Science & Artificial Intelligence, AIT Austrian Institute of Technology, Austria

Panelists

Katharina Schell
Deputy Editor-in-Chief, APA – Austria Press Agency, Austria

Friedrich Moser
Austrian Documentary film producer & director, Director of the Movie "How to build a Truth Engine", Austria

Robert Moro
Researcher at the Kempelen Institute of Intelligent Technologies (KInIT) located in Bratislava, Slovakia

Georgios Kolliarakis
Coordinator EU P2P Global Dual-Use Programme, Foreign Policy Instrument/ European External Action Service (EEAS), EU

Julia Haas
Advisor to the OSCE Representative on Freedom of the Media (OSCE RFoM)

The session examined the evolving challenges of disinformation and its societal impact in the digital age, with a particular focus on journalism, technology, security policy, and democratic resilience. The discussion traced the shift from early debates on "fake news" and fact-checking toward a broader understanding of disinformation as part of the structural disruption of the media ecosystem. The growing role of AI was highlighted as a key driver of change, not only by lowering the barriers to producing false or misleading content, but also by transforming how information is accessed, prioritised, and trusted. AI-driven search and conversational systems were discussed as reducing the visibility of traditional journalism, raising fundamental questions about the future role of media and the need for journalists to actively shape, rather than merely react to, these transformations.

The panel discussion explored information integrity and disinformation from multiple disciplinary perspectives, including media, filmmaking, research, security policy, and law. The psychological and social mechanisms that make individuals and societies vulnerable to disinformation, conspiracy narratives, and populism were discussed, alongside the role of storytelling and media literacy in addressing these dynamics. The discussion emphasised that disinformation is not only a technological problem, but one rooted in social behaviour, trust, and power relations at the intersection of technology, politics, and society.

The societal harms associated with disinformation were examined in detail, including its potential to incite violence, undermine democratic institutions, and fuel xenophobic or extremist narratives. At the same time, the discussion highlighted the legal and operational challenges of responding to disinformation, particularly where content remains protected under freedom of expression. The cross-border nature of disinformation campaigns was identified as a critical issue, reinforcing the need for international cooperation and coordinated responses, especially in law enforcement and security contexts. Reference was made to EU-level research initiatives aimed at supporting authorities in addressing disinformation linked to crime and extremism.

From a policy perspective, the discussion addressed the difficulty of assessing and measuring the societal impact of disinformation. Links were drawn between cyber-related risks, polarisation, and interstate conflict, as reflected in global risk assessments. An emerging EU framework, the European Democracy Shield, was discussed as an overarching approach to strengthening democratic resilience against disinformation, with further development anticipated in 2025. A central challenge identified was the ability to trace and quantify the progression from online disinformation to offline harm, which is essential for evidence-based policymaking and effective law enforcement. Variations in the availability and granularity of national data were noted as a significant barrier to comparative analysis and systemic understanding across countries.

The discussion concluded with a broader societal and legal reflection on the long-term implications of disinformation. While disinformation itself is not a new phenomenon, its scale, speed, and reach in the digital environment were described as unprecedented. Building resilience was framed as a systemic task requiring a combination of regulatory safeguards for media freedom, pluralism, and transparency; sustained support for public interest journalism; and international, multi-stakeholder cooperation. Audience engagement reinforced concerns around European digital sovereignty, with emphasis placed on reducing dependency on non-European private platforms and on developing decentralised, public-interest-oriented alternatives as part of a comprehensive response to disinformation.

Session 12

The Fight for Democracy: Censorship vs. Free Speech and Fact-Checking

Chair

Sabine T. Köszegi
Head of the Institute of Management Science, Technical University Vienna, Austria

Panelists

Carmen Isabel Grabuschnig
Guest Lecturer, University of Sorbonne: A new love for censorship? How social media and identity politics undermine the fundamental values of democracy, France

Filimon Peonidis
University Professor for Philosophy at the Aristotle University Thessaloniki, Greece

Anis Bajrektarevic
Professor, Board Member of IFIMES, Slovenia

Nico Hornig
Research Associate at the chair of Economic Policy Journalism at TU Dortmund and research associate at GADMO (German Austrian Digital Media Observatory), Germany

Viacheslav Riabtsev
Administration of the State Service of Special Communications and Information Protection of Ukraine, Associate Professor of Special Academic Department No. 5 of the Institute of Special Communications and Information Protection of the National Technical University of Ukraine, Ukraine

The session examined one of the most pressing challenges for democratic societies in the digital age: how to safeguard freedom of expression while effectively addressing misinformation, disinformation, and online manipulation. As digital technologies increasingly shape public discourse, the discussion focused on the tension between protecting open debate and responding to harmful content in ways that do not undermine democratic values.

The discussion opened with a philosophical reflection on the current state of freedom of expression in the digital sphere. Particular concern was raised about the expanding scope of censorship practices, not only by governments but also by private platforms, often justified through content moderation policies. These developments were discussed as raising complex legal and ethical questions, especially where measures intended to counter harmful content risk constraining legitimate expression and pluralism.

The panel explored the role of fact-checking as a cornerstone of democratic discourse. Independent fact-checking initiatives were discussed as essential for maintaining trust in factual information, with the erosion of such trust identified as a direct threat to democratic foundations. At the same time, the limitations of fact-checking as a standalone response were acknowledged, given the scale, speed, and sophistication of contemporary disinformation.

Historical perspectives on the relationship between technology and power were brought into the discussion, highlighting how digital tools have repeatedly reshaped political authority and social control. In this context, AI-generated deepfakes were identified as posing unprecedented risks to truth, civil liberties, and democratic accountability. The discussion emphasised the need for coordinated responses involving governments, civil society, and international institutions to counter emerging forms of digital authoritarianism.

The geopolitical dimension of digital manipulation was also addressed. Cyber warfare and information manipulation were discussed as integral components of contemporary geopolitical conflict, reinforcing the need for robust cybersecurity measures, resilient digital infrastructures, and trustworthy e-democracy tools to protect democratic institutions. Digital resilience was framed as both a technical and societal requirement.

From an academic perspective, the discussion examined changes in the understanding and practice of academic freedom. Generational shifts within universities were highlighted, alongside the observation that calls for censorship increasingly originate from within academic communities themselves. These dynamics were linked to broader social pressures, including anxiety, identity politics, and the amplifying effects of social media on public debate.

The session concluded with a discussion of mitigation strategies that extend beyond fact-checking alone. A combination of comprehensive media and digital literacy initiatives, strengthened professional journalism standards, effective AI regulation and platform accountability, and the protection of academic and expressive freedoms was identified as essential. Cross-sector and international cooperation were emphasised as necessary to uphold democratic values in an increasingly fragmented information environment. Overall, the discussion underscored the urgency of balancing freedom and security at a time when the concept of truth itself is under growing pressure.

Social Science Track Session 1

Digital Sovereignty or Digital Illusion? Power, Governance, and the Politics of Controlling Big Tech

Chair

Victoria Kontrus
Researcher at VICESSE | Vienna Centre for Societal Security

Panelists

Bart Karstens
Rathenau Institute, Royal Dutch Academy of Arts and Sciences: Are the Dutch taming Big Tech?, Netherlands

Komitas Stepanyan
Technology, Information & Cybersecurity Director, Central Bank of Armenia
American University of Armenia: The New Digital Borders: Cloud Infrastructure, Cybersecurity, and the Future of Sovereignty, Armenia

Mari Galstyan
American University of Armenia: The New Digital Borders: Cloud Infrastructure, Cybersecurity, and the Future of Sovereignty, Armenia

Plixavra Vogiatzoglou
Postdoctoral researcher at Universiteit van Amsterdam: Digital sovereignty's legitimising role: the case of the European Union, Netherlands

This session critically examined the promises and pitfalls of digital sovereignty in an era dominated by global technology giants. Through three complementary presentations, it explored how governments, public institutions, and supranational bodies attempt to assert control over digital infrastructures, data governance, and technological dependencies – and whether these efforts amount to genuine sovereignty or an illusion of control.

Bart Karstens (Rathenau Institute, Royal Dutch Academy of Arts and Sciences) presented a detailed case study of the Dutch education sector's negotiations with Google and Microsoft. While the resulting agreements improved transparency and mitigated key privacy risks, Karstens highlighted ongoing concerns about institutional dependency, regulatory gaps, and the burden placed on educators and users to maintain compliance. His talk questioned whether strategic negotiation is a viable path to digital autonomy or merely a temporary patch in an imbalanced relationship.

Komitas Stepanyan and Mari Galstyan (American University of Armenia and Central Bank of Armenia) then shifted the focus to the global stage, analysing how cloud infrastructure and cybersecurity are redrawing the boundaries of sovereignty. Their presentation emphasised the growing influence of U.S., Chinese, and European cloud providers, and unpacked how efforts at "digital solidarity" often reinforce new forms of strategic dependence. They posed key questions about whether sovereignty and interdependence can truly coexist, and how emerging digital alliances may be shaping a new geopolitics of control.

Plixavra Vogiatzoglou (University of Amsterdam) concluded with a critical analysis of the EU's digital sovereignty discourse. She argued that while the concept plays a powerful legitimising role in shaping policy and funding priorities, it often obscures unequal distributions of power and benefit – particularly between larger and smaller EU member states. Her presentation warned that the pursuit of sovereignty, framed as strategic autonomy, may in practice entrench dominance by a select few actors and technologies.

The session closed with a lively discussion on the tension between the rhetoric and reality of digital sovereignty. Participants debated whether current regulatory and policy frameworks are sufficient to meaningfully constrain Big Tech, or whether they perpetuate a governance model in which public institutions remain structurally dependent on the very actors they aim to control.

Social Science Track Session 2

Democratisation and Policy Recommendations in the Fields of Data Transparency and State Autonomy

Chair

Marion Neunkirchner
Researcher at VICESSE Research GmbH (Vienna Centre for Societal Security) Social Science (Social work, Sociology), Austria

Panelists

Gwendolyn Murphy
University of Delaware/IWM Fellows: An Energy Transition Critical Raw Material Repository, United States

Julie Klinger
University of Delaware/IWM Fellows: An Energy Transition Critical Raw Material Repository, United States

Kuangran Li
Assistant Researcher at Shanghai Academy of Social Sciences: Balancing Sovereignty and Transparency: Soft Law Approaches for Enhancing Sovereign Debt Data Governance in the Digital Era, China

Fabio Seferi
PhD Candidate – Italian National PhD Program in Cybersecurity – IMT School for Advanced Studies Lucca & University of Florence, Italy: Sandboxes as regulatory infrastructure, Italy

The session brought together three forward-looking contributions examining how digital governance frameworks can be designed to balance the competing demands of transparency, sovereignty, and democratic accountability in rapidly evolving technological and geopolitical contexts. The discussion focused on how governance design can address structural power asymmetries while enabling more inclusive and equitable forms of data management.

The first contribution examined the ethical, feasibility, and scalability implications of establishing a Central Energy Transition Critical Raw Material (ET-CRM) Data Repository. The proposed repository was discussed as a mechanism to enhance mineral transparency and traceability across supply chains in an ethical and lawful manner. Particular attention was given to issues of data sovereignty across physical, political, and social infrastructures, as well as to questions of social equity. The repository was framed as a potential space for counter-narratives of data sovereignty, with an explicit emphasis on challenging hegemonic knowledge paradigms in order to support more cooperative and equitable models of ecological governance.

The second contribution addressed the tension between increasing international demands for data transparency and the sovereign rights of states, focusing specifically on sovereign debt data governance in the digital era. Existing governance arrangements, largely shaped by non-binding guidelines issued by global institutions, were discussed as insufficient to meet the challenges of digitalisation. In response, the discussion explored soft law approaches as a pragmatic intermediary solution, capable of enabling gradual improvements in transparency while preserving national autonomy and decision-making authority.

The third contribution focused on regulatory sandboxes as emerging instruments of digital governance within new EU legislation. Rather than treating sandboxes solely as technical testing environments, they were discussed as evolving regulatory infrastructures that shape democratic participation and influence legislative development. The discussion emphasised the importance of broadening participation in the design and evaluation of sandbox programmes, including the involvement of civil society and advocacy organisations. Creating deliberative spaces that extend beyond purely commercial and technical interests was presented as essential to aligning digital experimentation with wider societal values.

Taken together, the contributions underscored the central role of governance design in protecting democratic values while maintaining state autonomy. The session highlighted the need for adaptive, participatory, and power-sensitive policy frameworks that recognise the political dimensions embedded in digital infrastructures. Overall, the discussion offered practical policy-oriented reflections for institutions, regulators, and states navigating the complex interplay between data transparency, sovereignty, and democracy in the digital age.

Keynote

A New Love for Censorship? How Social Media and Identity Politics Undermine the Fundamental Values of Democracy

Keynote

Carmen Isabel Grabuschnig
Guest Lecturer, University of Sorbonne:
A new love for censorship?
How social media and identity

This keynote explored how the dynamics of social media and the rise of identity politics simultaneously threaten freedom of expression and democratic values.

Carmen Grabuschnig began by retracing the emergence of cancel culture in American universities, illustrated by the 2015 Halloween costume controversy at Yale's Silliman College. Universities – once spaces for intellectual debate – have increasingly prioritised "safe spaces". As a result, many progressive students now view speech as potentially violent and suppress opposing views. Surveys confirm a rise in self-censorship and fear among students, while administrators reinforce this trend with lists of "microaggressions" and trigger warnings.

A comparison with France shows that, although similar tendencies exist, generational divides are less pronounced, and cancel culture is less pervasive. Members of Generation Z and Millennials broadly value free speech, though many still support restrictions on racist, misogynistic, or false content.

Drawing on the works of Jonathan Rauch, Carmen Grabuschnig distinguished between critical debate – essential in academia – and cancel culture, which seeks punishment rather than dialogue. Six markers of cancel culture's destructive nature were identified: punitiveness, deplatforming, organisational coordination, secondary boycotts, moral grandstanding, and "truthiness."

Tracing its roots, she argued that overprotective parenting and the rise of a "phone-based childhood," as described by Jonathan Haidt, have weakened Generation Z's resilience. Heavy social media use amplifies risks of addiction and insecurity through constant comparison with others, while algorithms reward sensationalist and polarising content. Together, these factors accelerate political radicalisation, reinforcing tribalism and intolerance.

According to Carmen Grabuschnig, identity politics undermine inclusiveness by emphasising group differences and fostering zero-sum struggles for recognition. Rather than empowering minorities, these developments risk deepening existing divisions. Genuine inclusivity, she argued, requires universal principles rather than fragmented group identities.

In conclusion, Carmen Grabuschnig called for strengthening resilience in future generations by promoting free, unsupervised play and delaying exposure to social media. Autonomy must be rebuilt through trust, mutual consideration, and transparent digital infrastructures. Quoting Timothy Garton Ash, she emphasised the need to learn how to "cope with difference" and to defend open debate in increasingly diverse societies.

Discussion: Propaganda, Disinformation and Digital Security

Chair

Matthäus Vobruba
Financial Officer at VICESSE Research GmbH, Austria

Panelists

Carmen Isabel Grabuschnig
Guest Lecturer, University of Sorbonne: A new love for censorship? How social media and identity politics undermine the fundamental values of democracy, France

Nico Hornig
Research Associate at the chair of Economic Policy Journalism at TU Dortmund and research associate at GADMO (German Austrian Digital Media Observatory), Germany

Roger von Laufenberg
Managing Director Vienna Centre for Societal Security VICESSE, Austria

The session examined how the digital age has transformed propaganda and disinformation, and what these changes mean for academia, society, and digital security. The discussion focused on the evolving nature of influence operations, the vulnerabilities created by digital environments, and the implications for research, governance, and resilience.

A central theme was the comparison between traditional forms of propaganda and contemporary digital disinformation. Classic state-driven propaganda was described as relying on hierarchical control structures, limited broadcast channels, and identifiable sources. In contrast, digital disinformation operates within decentralised and often anonymous ecosystems, where influence is diffused across platforms, networks, and users rather than directed from a single centre.

The discussion addressed the question of whether societies have become more vulnerable under these conditions. The prevailing view was nuanced. On the one hand, digital disinformation campaigns increasingly exploit cognitive biases and benefit from algorithmic amplification, with content rewarded for engagement rather than accuracy. Emotions such as outrage, fear, and polarisation were described as being systematically prioritised, while many users struggle to critically assess the information they encounter. On the other hand, it was also noted that access to information is broader than at any previous point in history, complicating simplistic assessments of vulnerability.

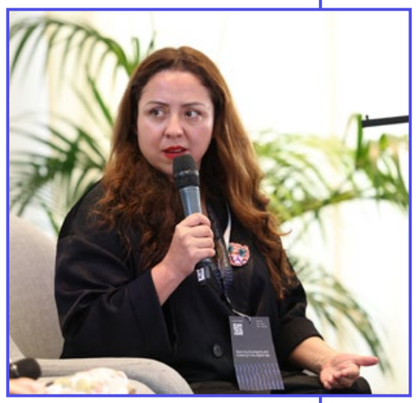
Attention then turned to the academic sector and its role within this environment. Research on propaganda and disinformation was discussed as carrying inherent dual-use risks, where scholarly work intended to analyse or counter manipulation may itself be repurposed for harmful ends. This raises ethical challenges for researchers, who must balance openness, transparency, and reproducibility against the risk of misuse. The discussion highlighted the need for robust research governance frameworks and a renewed emphasis on academic integrity to navigate these tensions responsibly.

The session further explored how propaganda itself has evolved in the digital age. Rather than remaining a purely top-down practice, propaganda was described as increasingly participatory, interactive, and often AI-generated or AI-assisted. Users play an active role in amplifying manipulative narratives, sometimes unknowingly, while the speed and scale of dissemination have expanded dramatically through digital platforms and automated tools. These dynamics were identified as significantly complicating efforts to detect, counter, and regulate disinformation.

Overall, the discussion underscored that propaganda and disinformation are no longer marginal or purely informational challenges, but central issues for digital security and societal resilience. Addressing them requires a combination of critical literacy, ethical research practices, and governance approaches that reflect the realities of a digitally networked public sphere.

Workshop

Digital Sovereignty in a Connected World: Navigating Between Openness and Control



Chair

Daniela Pieters
Technology Expert, Vienna Business Agency, Austria

Stephanie Jakoubi
Head of the Strategic Partnership Management, Communication, and Events, SBA Research, Austria

Panelists

Claudia Reinprecht
Head of Department for Telecommunications, Digital and Tech Diplomacy, Austrian Ministry for European and International Affairs, Austria

Carina Zehetmaier
CEO paiper.one, Member of the Austrian AI Advisory Board at Digital Austria, Austria

Plixavra Vogiatzoglou
Postdoctoral researcher at Universiteit van Amsterdam: Digital sovereignty's legitimising role: the case of the European Union, Netherlands

Salmi Ahsan
Security Solution Advisor, SAP Berlin, Germany

Renata Ávila Pinto
CEO of Open Knowledge Foundation, United Kingdom

Against the backdrop of growing geopolitical tensions, escalating cyber threats, and increasing dependencies on dominant technology providers, the workshop examined digital sovereignty as a central strategic challenge for Europe and beyond. As reliance on foreign IT systems and on the goodwill of large technology companies deepens, the urgency of building resilient, secure, and sovereign digital ecosystems has become more pronounced.

The workshop explored how the European Union and its institutions are rethinking digital infrastructure, data governance, and strategic autonomy. Particular attention was given to the role of international cooperation, trust-based governance, and shared standards in balancing national control with global connectivity. The discussion focused on what is required to shape a digital future that is not only secure, but also fair, inclusive, and sustainable.

Moderated around the guiding question of whether Europe can keep pace in the pursuit of digital sovereignty, the discussion brought together perspectives spanning digital diplomacy, law, research, cybersecurity, human rights, data governance, and intellectual property. Digital sovereignty was approached as a multidimensional concept encompassing the protection of infrastructure and data, ethical and legal accountability, and the societal dimension of empowering citizens through knowledge, trust, and participation.

Several core themes emerged during the interactive exchange. The costs of digital transformation were discussed not only in financial terms, but also with regard to ethical and social implications. Questions were raised about who ultimately benefits from digital sovereignty initiatives and who bears their burdens. The discussion further addressed how geopolitical developments, including the war in Ukraine and the technological rivalry between the United States and China, are reshaping Europe's digital environment. In this context, resilience was framed as something that must be achieved through cooperation rather than isolation, with calls for Europe to pursue new and diversified partnerships, including with actors in the Global South.

Europe's existing strengths were identified as a key strategic asset. Established frameworks in data protection, digital rights, and research excellence were discussed as providing a strong foundation for leadership in ethical technology development. The challenge, however, was described as one of implementation: acting with confidence, coherence, and the willingness to translate principles into practice.

The workshop concluded with a shared reflection that Europe's path toward digital sovereignty is defined less by speed than by strategy, inclusion, and resolve. Investing in people, fostering trust, and building interoperable and ethical systems were identified as essential elements. Digital sovereignty was framed not as a race, but as a collective vision for Europe's future, grounded in existing knowledge, innovation ecosystems, and values. Digital and future literacy were highlighted as foundational prerequisites for achieving meaningful and lasting sovereignty.

Workshop

AI for Peace: The Promise and Peril of AI-Powered Engagement in Conflict Zones

Chair

Michele Giovanardi
Programme Officer, Digital Peacemaking, CMI — Martti Ahtisaari Peace Foundation, Finland

Felix Kufus
Advisor, Digital Peacemaking & Emerging Technologies, CMI — Martti Ahtisaari Peace Foundation, Finland

On 14 June 2025, the CMI – Martti Ahtisaari Peace Foundation hosted a 90-minute workshop at the International Digital Security Forum in Vienna to explore the use of artificial intelligence (AI) in peacebuilding. Facilitated by Michele Giovanardi and Felix Kufus, the interactive session examined how AI can expand participation in fragile contexts, while simultaneously raising important questions related to bias, data security, and representation.

The workshop opened with an overview of CMI's approach to digital peacemaking, which integrates digital tools to support—rather than replace—traditional mediation and dialogue processes. This approach includes the use of AI to analyse large volumes of qualitative data, reach remote constituencies, and complement in-person engagement, all underpinned by strict ethical standards and strong contextual safeguards.

A central focus of the session was a recent field case from Yemen. Between January and March 2025, CMI conducted a youth consultation using a WhatsApp chatbot that collected text and voice responses from 142 participants across all 18 governorates, achieving 36.8% female participation and a 94.5% completion rate. Inputs provided in Yemeni Arabic were transcribed, translated, and processed using the "Talk to the City" AI tool, enabling the identification of shared visions, obstacles, and opportunities for youth engagement in the peace process.

At the close of the workshop, participants took part in a real-time Mentimeter poll to reflect on the discussion. When asked to share their initial associations with "AI in peace and security," the most frequently cited terms were bias, inclusion, surveillance, and hope, reflecting both the promise and the risks of these technologies. Participants identified the greatest potential value of AI in three areas: amplifying marginalised voices, analysing qualitative data at scale, and monitoring emerging risks in online environments. At the same time, the main concerns raised related to algorithmic bias, limited transparency, and the potential misuse of data in repressive contexts.

Participant reflections echoed these themes. One reflection highlighted the risks of relying on automated tools for deeply human processes such as dialogue, while another pointed to the promise of the Yemen case alongside a desire for greater clarity on how local actors are involved in interpreting AI-generated outputs.

The workshop concluded with broad agreement that AI can play a constructive role in peacebuilding, particularly in contexts where physical access is constrained. However, its deployment must be carefully governed. Transparency, local ownership, and critical human oversight were identified as essential conditions for ensuring that AI is used ethically and effectively in the service of peace.

For further information, please contact:

Michele Giovanardi
michele.giovanardi@cmi.fi

Felix Kufus
felix.kufus@cmi.fi

Workshop

Artificial Intelligence and Cyber Security of High-Risk Critical Infrastructure

Chair

Sarah Case Lackner
Senior Fellow, Vienna Center for Disarmament and Non-Proliferation (VCDNP), Austria

Panelists

Szilvia Tóth
Cyber Security Officer, OSCE Secretariat, Transnational Threats Department, Austria

Daniele Sangion
CSO, Head of Digital Transformation Office, UniCredit Bank Austria, Austria

Stefan Brandl
Information Assurance Director at Austrian State Printing House, Austria

Rodney Busquim
Head of the Information Management Section, Division of Nuclear Security, Department of Nuclear, Safety and Security, International Atomic Energy Agency (IAEA)

This interactive workshop focused on the security implications of artificial intelligence for critical national infrastructure and explored how emerging AI capabilities are reshaping both defensive and offensive cyber operations.

The discussion addressed the growing threat of AI-enhanced cyber attacks targeting high-risk critical infrastructure, including attempts to compromise confidential data and disrupt key systems. Alongside these risks, the increasing relevance of cybercrime directed at critical infrastructure operators was highlighted. An interactive exercise involving the audience identified a set of shared concerns among security professionals, which then formed the basis for deeper discussion. Among these concerns were the hype surrounding the capabilities of new AI models and the ways in which AI may open novel pathways for cybercrime.

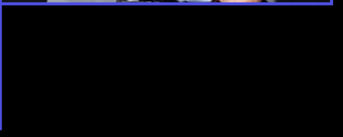
A recurring theme throughout the workshop was the need for systematic capacity building across all critical infrastructure sectors. Strengthening the ability to detect, prevent, and respond to AI-enabled cyber threats was discussed as essential. AI was examined both as a tool that can be exploited by adversaries and as a resource that can support earlier detection and improved analysis of cyber attacks. In this context, the shortage of experts with the skills required to apply AI responsibly and effectively in critical infrastructure protection was identified as a key challenge.

The discussion also highlighted the geopolitical dimension of AI-enabled cyber risks. Questions of responsible state behaviour in cyberspace were raised, underlining the importance of international dialogue and shared norms when addressing threats to critical infrastructure that often transcend national borders.

From an operational perspective, the workshop emphasised the importance of caution and vigilance when deploying AI tools in critical infrastructure environments. While AI can deliver clear efficiency and security benefits, participants stressed the need to remain aware of how the same technologies can be leveraged by malicious actors. Particular attention was given to the implications of AI models for social engineering, user manipulation, and fraud, as well as to the fact that AI-enhanced cybercrime is already occurring, especially within the financial sector.

The workshop concluded with a shared assessment that AI will simultaneously strengthen cyber security capabilities and expand the attack surface available to adversaries. Maintaining situational awareness of the evolving threat landscape and continuously adapting cyber security strategies were identified as essential requirements for safeguarding high-risk critical infrastructure in the years ahead.

Impressions
IDSF 2025



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 · Wirtschaftsagentur Wien Für die Stadt Wien Kofinanziert von der Europäischen Union · inno·x network · OVE Österreichischer Verband für Elektrotechnik · 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 · Wirtschaftsagentur Wien 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 · Wirtschaftsagentur Wien Für die Stadt Wien Kofinanziert von der Europäischen Union · X-NET

MEDIA

The Diplomatic Insight · CD Cercle Diplomatique · New Business · Report · IT WELT.at · Sicherheit

IMPRINT

Publisher / Editor:
AIT Austrian Institute of Technology GmbH
Giefinggasse 4, 1210 Vienna, Austria, ait.ac.at

Design: WHY. Studio
Photos Main Sessions: Katharina Schiffl
Photos Social Science Track: Valerie Maltseva/Agenda Studio

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.

INTERNATIONAL DIGITAL SECURITY FORUM *VIENNA*

www.idsf.io