Security Network Munich

CONFERENCE REPORT

MCSC MUNICH CYBER SECURITY CONFERENCE 2025

www.security-network-munich.org

THIS CONFERENCE WAS ORGANISED BY:

Peter Moehring
Managing Director
Security Network Munich

Charlotte Kobel
Security Network Munich

Rebecca Freymann
Giesecke+Devrient

INVALUABLE CONTRIBUTIONS BY:

Oliver Rolofs
Co-Founder MCSC,
Founder and Managing
Partner of COMMVISORY

Vivian Schiller
VP and Executive Director
at The Aspen Digital

Sasha O'Connell
Senior Director, Cybersecurity
Programs, Aspen Digital

Jeff Moss
Founder of DEF CON

John Mengers
Founder and Executive
Director of C-Suite Advisors

AUTHORS:

Stormy-Annika Mildner
Executive Director Aspen Institute Germany

Dr. Stormy-Annika Mildner (M.Sc.) became Director of the Aspen Institute Germany in Berlin, a renowned policy-oriented thinktank focusing on transatlantic relations and issues of global importance. As an adjunct professor, she teaches political economy at the Hertie School. From 2014 to 2020, she served as head of the department "External Economic Policy" at the Federation of German Industries (BDI), where she was responsible for international trade and investment issues. As Sherpa, she spearheaded the German Business7 Presidency (2015) and the German Business20 Presidency (2016-2017). Furthermore, she actively contributed as Co-Chair of Task Force Seven during the T20-Summit 2023 held in New Delhi and spoke at the Think7 Japan Summit 2023. Prior to joining BDI, she was Member of the Board of the German Institute for International and Security Affairs (SWP), worked as a lecturer at the John F. Kennedy Institute of the Free University of Berlin, and headed the program "Globalization and the World Economy" at the German Council on Foreign Relations (DGAP). She completed research fellowships at the American Institute for Contemporary German Studies and the Transatlantic Academy of the German Marshall Fund in Washington. She earned a Master of Science in international political economy from the London School of Economics and a PhD in economics from Freie Universität Berlin. During her doctoral studies, she conducted a one-year fellowship at the Yale Center for International and Area Studies (YCIAS) at Yale University.

Molly Hall
Senior Program Officer in the Digital Program the Aspen Institute Germany

Molly Hall is a Senior Program Officer in the Digital Program the Aspen Institute Germany where she manages projects focused on cybersecurity, AI governance, and digital policy. She brings more than a decade of public affairs, strategic communications, and public policy experience to the role. Her research interests include cybersecurity policy, international digital governance, and transatlantic tech relations. Prior to joining Aspen Germany, Molly was a consultant in Washington, D.C., helping clients create compelling communications and advocacy campaigns that impacted policymaking at the federal, state, and local levels. Molly holds a B.A. in International Relations and German from Michigan State University and a Master of Public Policy from the Willy Brandt School of Public Policy at the University of Erfurt.

This report was also developed with the support of Emilie Decker.

Emilie Decker
Project Assistant at the Aspen Institute Germany

Emilie Decker recently worked as a Project Assistant at the Aspen Institute Germany. She holds a B.A. in Social Sciences from Sciences Po Paris, where she focused on French-German and European Studies, and is currently completing her Master's degree in International Governance and Diplomacy with a concentration in Asian Studies. She previously gained experience at the Council of Europe in Strasbourg on the Reykjavík Process and the Environment, and at ARTE in the editorial office of Thema & Geopolitik. In 2023, she co-founded the German Student Association at Sciences Po Paris, where she lead communications and helped organize panel discussions and networking events for students. Among her diverse interests are diplomacy, feminist foreign policy, international security, and global governance in the digital age.

MCSC

MUNICH CYBER SECURITY CONFERENCE 2025

Uncertainty on the Rise:

Defining Purpose with Clarity!

Patronage:

Bavarian Ministry of Economic Affairs, Regional Development and Energy

Supported by:

AIRBUS, paloalto NETWORKS, Giesecke+Devrient Creating Confidence, Recorded Future, SIEMENS, Google, Meta, aws, TikTok, Allianz, Microsoft, Infineon, Lenovo, BRUNSWICK, Mastercard, schwarz digits, WITH secure, accenture, GitLab, EY Building a better working world, SIDLEY, CLOUDFLARE, Dataminr

Institutional Partners:

Bundesamt für Sicherheit in der Informationstechnik, msc Munich Security Conference, Alliance 4Europe, bitkom, DGAP Advancing foreign policy. Since 1955., DEFCON, SPRIN-D, Aspen Institute Germany, CSSA Cyber Security Sharing & Analytics, ASPEN DIGITAL aspen institute, SWP, German Mittelstand, NIKKEI, Business Software Alliance, Keidanren Policy & Action, BDI, Charter of Trust, EnSure collaborative, invest in bavaria, ISF, WOMEN 4CYBER, HPI Hasso Plattner Institut Digital Engineering · Universität Potsdam, ECSO EUROPEAN CYBER SECURITY ORGANISATION, UNITED EUROPE competitive and diverse, DIGITALEUROPE

EXECUTIVE SUMMARY

The cybersecurity landscape in 2025 is marked by unprecedented volatility. A rapidly fragmenting geopolitical order, the accelerated adoption of disruptive technologies, and the persistent shortage of skilled cyber professionals are together amplifying the sense of instability surrounding cyberspace.

Cyber risks are no longer episodic disturbances but persistent, strategic challenges with global repercussions. According to the World Economic Forum's Global Cybersecurity Outlook 2025 72 percent of respondents to its Global Cybersecurity Outlook Survey observed an increase in cyber risks. Ransomware was once again identified as the leading threat, with 45 percent of respondents naming it as their primary concern. In addition, the creation of deepfakes, which generate realistic images, audio, or video that impersonate real people, is also expanding exponentially. State-sponsored actors, particularly from Russia, China, Iran, and North Korea, have intensified their efforts against critical infrastructure, democratic institutions, and public trust, while influence campaigns seek to polarize societies and undermine democratic cohesion.

While the cybersecurity landscape remains complex and dynamic, it is also marked by significant progress. Advances in artificial intelligence (AI) and other emerging technologies, the strengthening of public-private partnerships, and rising societal awareness of cyber risks are contributing to a more resilient digital environment. Many organizations are now rethinking their security architectures, adopting integrated AI-driven solutions to address talent shortages, counter increasingly sophisticated adversaries, and reduce operational complexity.

Against this backdrop, the 2025 Munich Cyber Security Conference convened under the theme "Uncertainty on the Rise: Defining Purpose with Clarity!" to provide orientation in this unsettled terrain. Over two days, leading experts from government, industry, and academia examined how to confront the most pressing threats, seize the opportunities of innovation, and build resilience across borders and sectors. This report distills the essential insights, debates, and recommendations that emerged from the conference – offering both a sober assessment of the risks ahead and a roadmap for collective action.

The discussions revealed that the threat environment is deeply geopolitical. Cyber capabilities have become instruments of power projection, offering authoritarian regimes cost-effective tools of disruption that blur the boundaries between peace, crisis, and war. The attacks on civilian infrastructure, from hospitals to transport networks and energy grids, demonstrate how traditional lines between military and civilian domains are vanishing. NATO and EU members are adapting by treating cyberspace as a core operational domain, while national models such as Estonia's Cyber Defense League and Finland's Comprehensive Security Model underscore the value of a whole-of-society approach, integrating government, private sector, and civic expertise.

Equally important is the role of people. For decades, the dominant narrative has cast humans as the weakest link in cybersecurity, yet the MCSC underscored that, when empowered, they are a decisive strength. Education and cyber literacy, from schools to workplaces, are essential not only to reduce human error in increasingly complex systems but also to foster resilience against disinformation, deepfakes, and influence campaigns. Closing the cyber skills gap will require more diverse recruitment pipelines, inclusive workplace cultures, and the recognition that trust, transparency, and solidarity are as vital to defense as technical barriers.

The conference also emphasized that resilience cannot be achieved by planning alone. Written strategies and compliance frameworks are necessary but insufficient in the face of adversaries who move faster, exploit interdependencies, and target the weakest links. Real resilience requires practice: regular, large-scale exercises that test coordination, communication, and decision-making under live pressure. National simulations such as Germany's LÜKEX, NATO's Locked Shields, and EU-wide crisis drills have shown the value of bringing public and private actors together, yet small and medium-sized enterprises remain vulnerable and must be better integrated into resilience-building efforts.

Finally, the conference underlined that cybersecurity has no borders. Malicious actors operate fluidly across jurisdictions, exploiting regulatory divergence and the gaps between national mandates and international realities. Transatlantic cooperation remains indispensable but is challenged by differences in regulatory philosophy, particularly in areas such as platform accountability and AI governance. To narrow the gap between global threats and fragmented responses, governments and institutions must move beyond principles to interoperable systems, harmonized frameworks, and sustained cooperation.

The central message of the 2025 Munich Cyber Security Conference is clear: while uncertainty in cyberspace is rising, resilience and clarity of purpose are achievable. Meeting the challenge requires treating cyber defense as a strategic, societal and global endeavor. It demands a shift from reactive responses to anticipatory resilience, from siloed approaches to integrated cooperation, and from viewing humans as liabilities to recognizing them as the cornerstone of digital security. Only through such a comprehensive and inclusive approach can cyberspace remain not a theater of instability, but a foundation for innovation, prosperity, and democratic security.

KEY TAKEAWAYS

› Cyber Defense Must Keep Pace with a Shifting Threat Landscape

The cyber threat environment is no longer characterized by isolated incidents – it is now persistent, strategic, and increasingly geopolitical. Cyberattacks caused an estimated 8.4 trillion USD in global economic damage in 2022 (IMF). These losses are not limited to ransomware payouts or financial fraud. Instead, they also encompassed the cascading consequences of operational disruption, data theft, reputational damage, and efforts to rebuild trust after an incident.

According to the European Union Agency for Cybersecurity's (ENISA) 2024 report, the EU experienced unprecedented levels of cyber threats from a growing number of actors, with 11,079 major incidents recorded from July 2023 to June 2024. These attacks targeted a wide range of essential sectors, most prominently public administration (nearly 20 percent of recorded attacks), the transportation sector (11 percent), finance (9 percent), digital infrastructure (8 percent), and manufacturing (6 percent).

The rapid advancement of AI-driven technologies in recent years has supercharged the speed and potency of cyberattacks, often leaving defenders struggling to keep up with the ever-evolving tactics of malicious actors. AI-driven cyberattacks leverage a wide array of techniques, from crafting highly convincing phishing emails (spear phishing) and voice phishing (vishing) to bypassing security defenses in real time and pinpointing system vulnerabilities with remarkable precision.

While most attacks have come from non-state actors motivated by financial gain, geopolitical conflicts have been a strong driver in the cyber threat landscape, and collusion between state and non-state actors has become increasingly common. Russian-affiliated attacks – both kinetic and cyber – in Europe quadrupled from 2022 to 2023, and nearly tripled from 2023 to 2024 (CSIS). State-sponsored malicious cyber actors have also found havens in China, Iran, and North Korea.

Beyond the actors and geopolitical drivers shaping the threat landscape, the attack surface itself has expanded dramatically due to the proliferation of connected devices. This is creating new vulnerabilities across sectors. The complexity of securing this landscape has been further heightened by the increasingly blurred lines between civilian and military digital infrastructure: airports, hospitals, transport networks, and data centers may be owned and operated by private entities, but their compromise could have immediate strategic consequences.

In addition, Foreign Information Manipulation and Interference (FIMI) campaigns have become a central feature of today's hybrid threat environment, aiming to misinform, sow confusion, and erode institutional trust. Unlike spontaneous misinformation, FIMI campaigns are generally orchestrated by foreign actors, who are often state-sponsored, and who exploit existing societal tensions to sow confusion, distrust, and polarization. The 2024 European Parliament elections offered a salient example of how FIMI tactics have been deployed. In the months before the vote, EU agencies tracked a surge of coordinated influence campaigns, many originating from Russian-aligned networks.

This shifting threat landscape means that cyber defense can no longer be treated as a purely technical matter. It is a strategic endeavor that should be aligned with foreign and security policy and grounded in awareness of geopolitical risk. Public and private institutions need to adopt dynamic models of resilience that combine real-time threat intelligence, cross-sector coordination, and anticipatory policy design.

› Civilian and Military Cyber Resilience: Two Sides of the Same Shield

The traditional boundary between civilian and military spheres has become blurred in the digital age. Today's adversaries do not necessarily draw lines between military targets and civilian infrastructure. Cyber threats routinely target hospitals and energy grids with the same precision and intent as military command centers.

The blurring of boundaries between military and civilian cyber spheres was starkly illustrated in February 2022. Just hours before the Russian invasion of Ukraine, a coordinated cyberattack on the U.S.-based satellite firm Viasat disrupted civilian internet services across Europe and simultaneously impaired military communications in several NATO member states.

NATO has moved decisively to acknowledge this threat convergence. Since 2016, cyberspace has been a declared operational domain, and the 2021 Brussels Summit reaffirmed the commitment to collective defense in the digital realm – which should include employing the full range of capabilities to deter, defend against and counter the full spectrum of cyber threats, including the potential application of Article 5, in the event that the impact of a significant malicious cyberattack constitutes an armed attack. In addition, NATO allies agreed to a new concept at the Vilnius Summit in 2023 to enhance NATO's overall cyber deterrence and defense posture, which included improving civil-military cooperation at all times.

Among NATO members, Estonia stands out as a global leader in cyber defense integration. After suffering a massive cyberattack in 2007 that paralyzed its public and financial services, Estonia invested heavily in national cyber infrastructure. It now hosts the NATO Cooperative Cyber Defence Centre of Excellence and is widely recognized as a top country in the EU for strong cybersecurity. What has made Estonia particularly notable is the Cyber Defence Unit of the Estonian Defence League – which is a novel means of organizing a voluntary corps of cyber professionals with the purpose of strengthening cyber skills to prepare and enhance support capabilities in times of crisis. This fusion of public expertise, private innovation, and national service reflects a whole-of-society defense posture (i.e. an integrated national security strategy that mobilizes all segments of society to collectively prepare for and address a broad spectrum of threats and challenges). Several other

European countries also follow a whole-of-society defense approach. One of them is Finland with its comprehensive security model, which fosters cooperation among all sectors of society – from defense and civil protection to telecoms and education. Regular cyber defense exercises at the local and national level form part of this approach.

The United States has also taken a more comprehensive approach to defending its cyberspace. The most recent National Cybersecurity Strategy, published in 2023, emphasized a "defend forward" doctrine, meaning to use offensive capabilities to disrupt adversaries before they strike. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has acted as a national coordinator, linking private companies and critical infrastructure operators with government agencies.

Across these examples, the lesson is clear: no modern security architecture can afford to treat cyber resilience as a purely military or civilian task. Instead, the future lies in cross-domain interoperability, legal clarity, and a shared security culture that reaches from the server room to the situation room.

› People Are the Strong – Not the Weak – Link, If They Are Empowered

For decades, the dominant mantra in cybersecurity has been that "humans are the weakest link." This notion has shaped how organizations design defenses: isolating users, limiting access, and automating trust. But this view has been somewhat reductive and potentially dangerous. In a world where threat actors have exploited human psychology alongside software vulnerabilities, the idea that people are liabilities has become a self-fulfilling prophecy. On the contrary, when equipped with the right tools, knowledge, and agency, humans are not the weakest link. They can be an adaptable, context-sensitive and resilient element of any security system.

The numbers confirm that human factors play an important role in many breaches. However, much of this is not due to negligence or incompetence, but prompted by increasing system complexity and insufficient training.

Cyber literacy is an important component of any training focus. For example, in Finland, media and digital literacy are taught beginning in primary school, with a complementary focus on safety and data protection. Correspondingly, Finland topped the European Media Literacy Index (published 2017 to 2023 by the Open Society Institute Sofia) since its inception in 2017, demonstrating a strong societal resilience to disinformation and misinformation.

Beyond awareness, empowerment requires agency. This could mean moving away from one-way messaging ("Don't click this") to participatory security cultures where employees, citizens, and service users are included in threat modeling and resilience planning. In organizations, this might mean co-developing security protocols with frontline staff. In communities, it could mean recruiting "cyber stewards" to support vulnerable populations. In government, it could mean embedding cyber considerations into every level of public administration.

Cyber empowerment also relies on using relatable language and simplicity to communicate with users. Reframing cybersecurity around values like resilience, responsibility, and solidarity would help build trust, which has been a vital component in the face of attacks that look to disintegrate social cohesion and discredit public institutions.

Finally, cyber empowerment needs to be about inclusion. Women, minorities, and older adults have remained underrepresented in cybersecurity professions and underserved in outreach campaigns. The global cybersecurity workforce is currently facing a shortfall of over four million professionals, yet less than 25 percent of that workforce is female according to the 2024 ISC2 Cybersecurity Workforce Study.

To ensure that people are the strong link in cyber defense requires a paradigm shift: from compliance to competence, from awareness to agency, from exclusion to inclusion. Only then a resilient, adaptive, and democratic cyber defense for our societies can be built.

› Crisis Preparedness Requires More Than Planning – It Requires Practic

There has been no shortage of national cyber strategies, sectoral guidelines, or risk registers. But as cyberattacks have become faster, more targeted, and more multidimensional, the true test of resilience lies not in planning alone, but in practice. Cybersecurity today is not just a matter of defense posture; institutions need to ensure that they are capable of the cross-sectoral cooperation and quick thinking that is required to respond in the moment.

Governments have started to act on this realization. Germany's crisis management LÜKEX exercises, for example, have matured into national-scale simulations involving federal ministries, municipalities, private operators, and increasingly, the military. Additionally, NATO's "Locked Shields" drill in 2024 brought together 4,000 participants to simulate advanced cyberattacks against real infrastructure, combining technical, legal, and communications challenges under live pressure.

Within this growing ecosystem of readiness, small and medium-sized enterprises (SMEs) play an important role. SMEs, however, are struggling with the cost and complexity of acquiring adequate cyber defense capabilities. The well-known reasons include: limited budgets, shortage of in-house expertise, reliance on legacy systems, and a perception that they were not high-value targets. Often, the attacks are not ends in themselves, but steppingstones to access larger companies, public institutions, or critical infrastructure.

Some progress has been made in addressing this challenge. In Germany, the Alliance for Cyber-Security (ACS), established in 2012 by BSI and Bitkom, a German digital association, offers free resources, webinars, and early-warning systems to more than 8,000 organizations, many of which are SMEs. Similarly, the United Kingdom's National Cyber Security Centre (NCSC) has provided tailored risk management tools, like the Cyber Essentials certification, to help smaller firms meet baseline standards without costly audits.

Cybersecurity requires ecosystems where every actor, no matter their size, knows their role and has the means to fulfill it. Diligent planning, incorporating as many business, sectors, and public actors as possible, will help to improve adaptability and readiness. Preparation should include crisis response exercises as well as education and communication opportunities to improve competence and interconnectedness.

› Cybersecurity Has No Borders – International Cooperation Is the Best Defense

The borderless nature of cyberspace has enabled threats to proliferate across jurisdictions, undermining national defenses and exploiting global connectivity. Ransomware, network intrusions, and disinformation campaigns unfold across platforms and languages, often with a speed and reach that exceed the capacity of states to respond effectively. This mismatch reflects a deeper structural tension: while threats operate globally, governance remains fragmented, shaped by national legislation, regional priorities, and asymmetrical capabilities. In this space of regulatory divergence, adversaries have found room to thrive.

Disinformation provides a telling example: it has rarely been confined to borders, and yet responses have remained uneven, with some governments framing it as a communication issue while others treat it as a systemic threat to democratic sovereignty. This divergence illustrates the difficulty of establishing a coherent international framework when political systems attach different weight to security, market freedom, and constitutional protections.

Divergences are becoming increasingly visible also across the Atlantic. The European Union is pursuing a comprehensive and binding regulatory approach, embedding cyber resilience into its legal architecture through initiatives such as the Digital Services Act and the Code of Practice on Disinformation. The United States, by contrast, has leaned on innovation, market resilience, and voluntary partnerships with industry. Constitutional traditions, particularly interpretations of the First Amendment, constrain direct government involvement in content moderation, leading to a preference for cooperative rather than coercive measures.

Despite these structural asymmetries, there have also been points of convergence. Both sides of the Atlantic have increasingly recognized that regulatory divergence can be exploited by hostile actors and that some degree of policy coherence is necessary to safeguard shared infrastructures and values. Comparative work on cyber incident reporting requirements and ongoing dialogues on harmonization reflect this shift, creating entry points for closer alignment of standards and practices. Beyond regulatory questions, cooperation has also deepened in response to direct cyberattack threats. Joint attribution of malicious campaigns, coordinated diplomatic responses to state-backed hacking, and intelligence exchanges through NATO and bilateral channels demonstrate that the transatlantic partners are willing to act together when confronted with tangible disruptions. These measures do not yet constitute a fully integrated defense architecture, but they represent meaningful progress in building collective deterrence and resilience.

At the multilateral level, similar tensions persist. The G7 has consistently reaffirmed commitments to democratic digital governance, but outcomes have rarely gone beyond declaratory principles. The G20 has been unable to advance meaningful cyber norms, reflecting geopolitical divisions between liberal democracies on one side and Russia and China on the other. Within the United Nations, years of negotiations yielded only modest progress, though in 2025 they culminated in the creation of a new Global Mechanism for Cyberspace, a permanent body designed to provide continuity in norm development, capacity building, and conflict resolution. Whether this institution can move beyond symbolic consensus remains to be seen.

The international community thus finds itself at a crossroads. Cyber threats have become systemic, global, and strategically consequential, while responses remain fragmented, uneven, and often reactive. The transatlantic relationship embodies both the challenge and the opportunity: it demonstrates the costs of divergence but also the potential for building convergent frameworks where values align. Narrowing the gap between the global reach of threats and the national or regional scope of responses will require more than declarations of intent. It demands legally sound cooperation, institutionalized mechanisms, and interoperable systems that together can transform shared principles into collective resilience.

WELCOME:

Claudia Eckert
Chairwoman Security Network Munich

In her opening statement, Claudia Eckert welcomed the participants to the 11th Munich Cyber Security Conference. She introduced this year's theme, "Uncertainty on the Rise: Defining Purpose with Clarity", explaining that the conference aimed to shed light on the current state of cybersecurity and to provide guidance in an increasingly complex environment. Against a backdrop of rapid technological change and a volatile geopolitical landscape, Claudia Eckert noted that the level of uncertainty in the cyber domain had grown significantly. She highlighted that emerging technologies like AI and quantum computing were having a clear impact on cybersecurity but also questioned if the industry was prepared to address the impact. She also mentioned that the different perspectives from government, industry, and the scientific community were relevant for identifying what the new frontiers in cybersecurity were and how they should be addressed.

Claudia Eckert explained that over the next two days, the conference would bring together perspectives from government, industry, and academia to address these challenges in depth. Discussions would focus on the readiness of industries to adapt to novel advancements, and on strategies to reinforce the resilience of critical infrastructure. Attention would also be given to the balance between cybersecurity regulations and national sovereignty, including discussing whether structured regulatory frameworks were necessary to ensure stability without hindering innovation. In closing, Claudia Eckert stressed that none of these issues could be addressed in isolation. Tackling them required cooperation across sectors and borders. She emphasized that the MCSC remained a unique platform for knowledge-sharing, trust building, and the joint development of strategies to navigate an era of rising cyber uncertainty.

> Claudia Eckert:
> "In the face of rising uncertainty, it is imperative to come together to share our knowledge, share our expertise, and share our perspectives on cybersecurity."

OPENING PANEL:

Uncertainty on the Rise: Where to Put the Focus in Cybersecurity in 2025?

Moderator: **Siobhan Gorman,** Partner and Cybersecurity, Data & Privacy Global Lead at Brunswick Group

Felix Barrio, Director General of INCIBE

Keiichi Ichikawa, Assistant Chief Cabinet Secretary & Deputy National Security Advisor at the Cabinet Secretariat of Japan

Sami Khoury, Government of Canada Senior Official for Cyber Security

Marko Mihkelson, Member of the Estonian Parliament, Chairman of the Foreign Affairs Committee

Annegret Bendiek, Senior Fellow at SWP, Germany

The opening panel addressed the central question of where strategic attention should be placed in cybersecurity in 2025, a year marked by growing uncertainty, geopolitical rivalry, and technological disruption. As the discussion unfolded, three interlinked priorities crystallized: the need to confront state-sponsored threats, the necessity to strengthen resilience through trusted cooperation, and the demand to leverage new technologies like AI, while controlling for their risks.

Marko Mihkelson set the tone by highlighting the learnings from the ongoing cyber conflict between Russia and the West. He stressed that cyberattacks had been a core tool in Russia's broader strategy alongside allies like China, North Korea, and Iran. In his view, Ukraine's success, both militarily and in cyberspace, was essential to safeguarding European security.

> Marko Mihkelson:
> "We have to understand that we cannot distinguish what is happening in the cybersphere to what is going on generally in geopolitical landscape today."

Keiichi Ichikawa continued this geopolitical thread, stressing that cybersecurity could not be separated from the wider strategic geopolitical competition. He pointed to covert and sophisticated operations, such as the Volt Typhoon intrusions which had compromised the IT environments of multiple critical infrastructure organizations in the United States. He also mentioned North Korean affiliated cryptocurrency thefts, which he stated were used to fund nuclear missile programs. Keiichi Ichikawa argued for more regional cooperation, earlier threat detection, and stronger alliances among like-minded nations to better counter such threats.

> Keiichi Ichikawa:
> "It's really important to make our cyber capabilities strong enough to defend our values and norms and international order."

From there, the conversation shifted to the widening scope of cyber threats. Sami Khoury noted that cyberattacks had been expanding beyond governments, with hacktivists and AI-driven disinformation targeting democratic processes and private sector entities, particularly in response to political events. In his view, urgent national priorities included protecting electoral infrastructure, countering the manipulation of public opinion, and increasing public awareness. Annegret Bendiek tied these points together from a European perspective. She highlighted Russian efforts to weaken support for Ukraine, China's preparations for geopolitical contingencies – such as conflict over Taiwan or other regional flashpoints –, and the relentless growth of ransomware and cybercrime as the key drivers of Europe's cyber threat landscape. Ransomware, she noted, remained especially dangerous for the health and telecom sector, while state actors increasingly partnered with criminal networks to amplify their reach. Finally, Felix Barrio revisited the importance of cooperation. He argued that enduring trust between public and private actors, built through joint training and regular intelligence exchange, was the foundation for resilience. Integrating private-sector expertise into resilience planning, especially given the vulnerabilities of global supply chains, was in his view indispensable.

In the final exchanges, the panelists converged on the view that AI would be pivotal in future cyber operations – a powerful asset for defense, but also a potent tool for attackers. They emphasized that success depended on pairing AI-driven capabilities with strong human oversight to preserve accountability and control.

In summary, the three key takeaways from the opening panel were:

- **Focus on countering state-sponsored threats:** 2025 cybersecurity priorities must address the broader geopolitical rivalry, particularly by supporting Ukraine and deterring authoritarian alliances.

› **Strengthen resilience through cooperation that builds trust:** Sustained international collaboration, proactive intelligence-sharing, and closing skills and capacity gaps across sectors are essential to withstand evolving threats.

› **Use AI as an asset, but never without human control:** Artificial intelligence will be central to cyber defense and offense, but effective use will require pairing automated tools with human oversight to ensure accountability and minimize risk.

Engaging the Private Sector or How Can PPPs be Successful?

Moderator: **Geoff Brown,** President and Chief Operating Officer at Arete

Miguel De Bruycker, Managing Director General of the Centre for Cybersecurity Belgium
Jim Higgins, CISO at Snapchat
Thomas Seifert, CFO at Cloudflare
Max Peterson, Vice President of Sovereign Cloud Amazon Web Services

The discussion in this session focused on how public-private partnerships (PPPs) can be more effective in strengthening cybersecurity, moving beyond formal statements of intent to tangible, sustained results. While the concept of PPPs is far from new, the speakers agreed that core challenges, especially in a shifting geopolitical landscape, remained: building trust, aligning government requirements with operational realities, and shifting from information sharing to active, joint defense. Asked to grade the success of PPPs on a 1-5 scale (with five being the best), the panelists ranged between a 2.5 and 3.5.

Miguel De Bruycker opened with examples from Belgium that illustrated how successful PPPs can be when collaboration was embedded into daily processes. He explained that citizens were encouraged to forward suspicious emails to a centralized government email address, where the information was analyzed. This enabled the blocking of malicious domains, often within 15 minutes, which resulted in about 90 percent of users in the

country being protected. Miguel De Bruycker further emphasized the importance of real-time intelligence sharing and cooperation between national cybersecurity centers and private entities, stating that trust and structured communication were key. He further described a program, made possible by updated legal frameworks, that scanned for the most exploitable vulnerabilities and alerted system owners before attackers could act.

Max Peterson built on this point, highlighting the experiences of Amazon Web Services' (AWS) in Ukraine. He explained that before and after the Russian invasion, AWS helped preserve the Ukrainian government's digital infrastructure, identified phishing campaigns from malicious actor groups such as APT29 (also known as Cozy Bear), and blocked malicious domains. He stressed that such partnerships worked best when they were flexible, allowing each side to contribute according to its strengths rather than forcing a one-size-fits-all approach.

> Max Peterson:
>
> "I think the key to [successful partnerships] has been coordination and collaboration on response. ... I think a lot of it is the structural underpinnings but then a lot of it just relies upon getting the relationship going and building the trust and confidence in the partners that you're working with."

The discussion then turned to what happens when collaboration falters. Thomas Seifert cautioned that PPPs could fail when governments prescribed technical solutions instead of letting industry innovate. Drawing on Cloudflare's defense of Ukrainian systems and its role in the joint response to the Log4j vulnerability, a critical flaw in a widely used open-source logging library that allowed attackers to remotely execute code, he argued that speed and trust were essential to resolving the problem. He argued that governments should focus on coordination rather than control. Jim Higgins added to this argument and explained that private companies often saw attacks unfold across their global infrastructure in real time but lacked the legal authority to disrupt them. Her argued for a "joint cybersecurity room," where public and private experts could work side by side, not only in crises but also during peacetime, to shorten reaction times and strengthen defenses.

> Thomas Seifert:
>
> "I think the most progress I saw in building up to these partnerships is actually moving transactional considerations to the side and leaning in, in order to achieve that first barrier of of trust."

To summarize, the three main takeaways from the discussion were:

- **Build trust and structured collaboration before crises:** Effective PPPs depend on established relationships, rapid information flows, and clear mechanisms for two-way intelligence exchange.
- **Align regulation with operational realities:** Streamlined, standardized frameworks should enable innovation and enable rapid, coordinated responses
- **Advance from sharing to doing:** Partnerships should evolve from exchanging information to joint, hands-on defense, supported by sustained investment in developing and retaining cyber talent.

SPOTLIGHT:

New Frontiers in Cyber Security

Moderator: **Ciaran Martin,** Professor at the Blavatnik School of Government, University of Oxford

Noboru Nakatani, Corporate Executive Vice President and CSO at NEC, Japan

Marco Obiso, Chief of Digital Networks and Environment Department, Telecommunication Development Bureau, ITU

Wendi Whitmore, SVP of Unit 42 at Palo Alto Networks

Oleksandr Potii, Chairman of SSSCIP of Ukraine

Nathaniel Gleicher, Global Head of Counter-Fraud and Security Policy, Meta

The spotlight session explored what the panelists considered the "new frontiers" of cybersecurity: the vulnerabilities of physical cyber infrastructure, the growing sophistication of cyber-enabled scams, and the transformative yet double-edged impact of AI. While the panelists detailed how these frontiers differed, the discussion revealed how they are intertwined by shared risks: concentrated points of failure, the complexity of interconnected systems, and the widening gap between attacker agility and defender response.

The discussion began by focusing on the first frontier that was identified: subsea internet cables, which carry over 95 percent of global internet traffic. Marco Obiso noted that in cybersecurity discussions, the physical infrastructure resilience had been rarely addressed. He argued that protection should focus on resilience through diversified routes, continuous monitoring, and stronger international legal safeguards. Noboru Nakatani added that cable ownership and control were highly concentrated, making the issue as much geopolitical as technical. He also warned that subsea cables were exposed to a wide range of risks, from natural disasters and accidental damage to eavesdropping and intentional interference. He stressed that building resilience required both physical and cyber protection measures. Oleksandr Potii added the human component of cybersecurity. He also emphasized that the private sector know-how was critical for strengthening government cyber resilience.

The next frontier to be discussed was the growing challenge of cyber-enabled scams, which Nathaniel Gleicher described as a global epidemic. He explained that these scams were increasingly sophisticated and supported by organized crime networks, affecting businesses and individuals. He stressed that these actors needed to be countered with the same persistence as state-sponsored attacks.

> Nathaniel Gleicher:
> "I would make the case that over time, AI has all the potential to be better for defenders than for attackers."

Finally, the panel discussed another challenging frontier, namely AI's evolving role in cybersecurity. Wendi Whitmore noted that AI had been increasingly aiding attackers, while also offering significant opportunities to strengthen defenses.

Nathaniel Gleicher agreed, adding that AI could be a greater asset for defenders if paired with strong governance and human oversight.

> Wendi Whitmore:
> "When we look at AI, and attackers in particular, I think what we're seeing to date is more evolutionary than revolutionary."

The panel concluded with a call for more effective international coordination and global governance in cybersecurity, noting that the significant gap in the speed of action between bad actors and governments needed to be improved. The panelists shared a sense of cautious optimism, rating their confidence in addressing these new frontiers at six out of ten.

The main takeaways from this discussion were:

- **Strengthen critical infrastructure resilience:** Address vulnerabilities in systems like subsea cables through route diversification, continuous monitoring, and legal safeguards.
- **Treat cyber-enabled scams as priority threats:** Counter them with the same persistence and coordination used against state-sponsored actors.
- **Use AI as a defensive advantage:** Leverage its scale and speed for protection, ensuring it is guided by clear rules, expert oversight, and cross-sector collaboration.







FIRESIDE CHAT:

Intelligence View

Moderator: **Chris Ahlberg,** Co-Founder and CEO at Recorded Future

Carl Bildt, Former Prime Minister of Sweden
Sir Jeremy Fleming, Former Head of UK Intelligence, Cyber and Security Agency, GCHQ
Dag Baehr, Vice President of Federal Intelligence Service (BND)

The fireside chat on intelligence and cybersecurity explored the rapidly changing dynamics of intelligence in response to global instability, technological advancements, and shifting political landscapes. The discussion began by analyzing how intelligence agencies are adapting to meet the increasing speed of information flows.

Carl Bildt remarked that political leaders increasingly expected intelligence to be delivered continuously, moving beyond the traditional model of periodic reporting.

Sir Jeremy Fleming explained that agencies had already become more operational but more needed to be done.

Dag Baehr then noted that the line between classified and open-source information was blurring, requiring agencies to integrate private sector capabilities and more operational, real-time assessments.

Carl Bildt:

"HUMINT has become very difficult indeed because of technological developments."

Sir Jeremy Fleming:

"Artificial intelligence does fundamentally change the nature of intelligence. It changes the nature of intelligence tasks because intelligence officers and agencies have different tools at their disposal to sift through information to bring the things that really matter to the top, to improve efficiency, and effectiveness."

Dag Baehr:

"There still is a role for human intelligence, as opposed to AI or any kind of SIGINT which is out there as well."

From there, the discussion turned to the future of intelligence in the age of AI. Sir Jeremy Fleming described AI as a major opportunity for defenders but acknowledged it would also be exploited by adversaries. Dag Baehr cautioned that the scale of AI-driven threats created resource and ethical challenges, while Carl Bildt underlined that most technological advances came from the private sector, making close cooperation indispensable.

Finally, the discussion shifted to Europe's position in the AI race. The speakers debated the continent's reliance on external technology and the strategic need to strengthen capacities and capabilities. The speakers emphasized that partnerships, especially with allies like the United States, were essential, but that Europe should be able to act from a position of technological strength rather than dependency. In closing, the panelists called for more frequent public debates about the role of AI and privacy in national security and underlined that public trust was essential to the legitimacy and effectiveness of European intelligence work.

The key takeaways from the discussion were:

- **Adapt intelligence for speed:** Provide continuous, operational insights that combine open-source and classified data into timely, actionable assessments.
- **Apply AI with balance:** Exploit its potential to strengthen defenses while ensuring accountability and preserving human judgment, particularly in interpreting intent.
- **Build public trust in Europe's intelligence:** Ensure transparency and maintain regular dialogue with policy makers, oversight bodies, and the public to balance security, privacy, and democratic legitimacy.




SECOND PANEL:

Human League: Leadership and Engagement for Managing Future Cyber Risks

Moderator: **Kiersten Todt,** Former Chief of Staff at CISA and President of Wondros

Paul M. Nakasone, Former NSA Director and Founding Director of the Vanderbilt University Institute of National Security

Peter Kant, Chairman and CEO at Enabled Intelligence

Ann Cleaveland, Executive Director of the UC Berkeley Center for Long-Term Cybersecurity

Johan Gerber, Executive Vice President and Head of Security Solutions at Mastercard

Natalia Oropeza, Global Chief Cybersecurity Officer at Siemens

The second panel explored what the speakers considered the most critical but often underestimated factor in cybersecurity: the human element. Unlike other sessions that focused primarily on technology or geopolitical

threats, this panel examined how people, skills, and culture shaped the ability to manage cyber risks in an uncertain and AI-driven world.

The discussion began by examining how the role of humans can be strengthened in the digital ecosystem. Johan Gerber argued that a shift from system-centric to consumer-centric security could strengthen the human role. He highlighted the growing convergence between scams and cybercrime and argued for "friction by design." According to him, these were safeguards that intentionally slowed down high-risk transactions, such as extra authentication steps or temporary holds, to give users time to confirm legitimacy. These measures, he argued, could enhance transparency, give users greater control, and build trust in digital interactions.

> Johan Gerber:
> "In a digitally connected world – and we will only get more digitally connected – I think there's this common agreement that every employee has to be part of cyber defense."

Picking up on the idea of designing systems with human needs in mind, Peter Kant and Ann Cleaveland both emphasized the need for diversity in the cybersecurity workforce. Peter Kant highlighted his company's hiring practices, arguing that cybersecurity talent pipelines should move beyond a narrow STEM focus and embrace diverse aptitudes and problem-solving approaches. He emphasized the necessity of critical thinking and adaptability in an AI-driven future. Ann Cleaveland then presented an innovative approach that had been taken at UC Berkley: cybersecurity-based clinics, modeled on the legal aid concept, where students from diverse educational backgrounds offered support to local organizations without dedicated IT staff. This, she noted, strengthened community resilience while giving students practical, socially relevant experience.

Linking the human factor to strategic capability, Paul M. Nakasone argued that professional development should combine technical fluency with strategic decision-making and strong communication skills.

Natalia Oropeza echoed this sentiment, emphasizing the need for leadership development, team empowerment, and the elimination of siloed thinking to foster a more agile cybersecurity environment. Furthermore, she argued that workplace culture needed to be strengthened by encouraging collaboration across teams, empowering staff, and building leadership capacity to respond quickly to new challenges.

> Natalia Oropeza:
> "Technologiy is not our problem... What I need, is help to develop my team, my people, my company, into agents of change to adapt to the many technologies – one of them is AI of course – in order for us to be faster."

The panel concluded with the shared view that people were not the "weakest link" but the decisive force in how effectively technology was used. Trust, they agreed, had to be built deliberately, diversity of thought had to be actively sought, and lifelong learning had to be embedded into organizational culture in order to successfully navigate future cyber risks and ensure that technology served society rather than the other way around.

The key takeaways included:

- **Put people at the center of cybersecurity:** Design systems that empower users, integrate safeguards that slow down high-risk actions, and build trust through transparency and control.
- **Broaden the definition of cyber talent:** Recruit across disciplines, cognitive profiles, and educational backgrounds to bring diverse problem-solving skills into an AI-driven security environment.
- **Strengthen workplace culture to drive resilience:** Foster collaboration, empower teams, and develop leaders who can adapt quickly to change in order to navigate future cyber risks.





SETTING THE SCENE

Catherine de Bolle

Executive Director of Europol

In her speech, Catherine de Bolle described the role of law enforcement in cybersecurity, warning that public trust in law enforcement could erode if cybercrime was not addressed decisively. Although cybercrime itself is not new, she emphasized that criminals increasingly blended traditional infrastructure abuse with advanced digital tools such as dark web services. The result was a threat environment that was faster, more interconnected, and harder to predict.

As an example, Catherine de Bolle cited the 2024 dismantling of the LockBit ransomware group. The operation spanned at least 10 countries, resulted in four arrests, two public indictments, and sanctions against two Russian nationals affiliated with LockBit. According to de Bolle, authorities seized 10 million EUR in cryptocurrency, froze or monitored 120 million crypto wallet addresses, and recovered more than 2,500 decryption keys. The case underscored the importance of cross-border cooperation and the critical role of law enforcement in confronting cyber threats at scale.

Looking ahead, Catherine De Bolle stressed that law enforcement had to continue investing in technical capabilities, prevention strategies, and victim support. She called for stronger partnerships with private industry and enhanced cooperation between civilian and military cyber communities. She also highlighted the need for modern legal frameworks and lawful pathways to access digital data in order to respond effectively to hybrid threats. Catherine De Bolle concluded by urging a shift away from fragmented approaches, emphasizing that multilateral collaboration was key to tackling the increasingly interconnected and hybrid nature of cyber threats.

> Catherine De Bolle:
> "Criminals will continue to adapt quickly and evolve and so must we: law enforcement."

Three takeaways from her speech were:

- **Scale up cross-border action:** Tackle criminal groups through coordinated arrests, sanctions and seizure of assets.
- **Broaden the definition of cyber talent:** Recruit across disciplines, cognitive profiles, and educational backgrounds to bring diverse problem-solving skills into an AI-driven security environment.
- **Strengthen workplace culture to drive resilience:** Foster collaboration, empower teams, and develop leaders who can adapt quickly to change in order to navigate future cyber risks.

HEAVY INFILTRATIONS:

Typhoon Talk – Law Enforcement Reloaded

Moderator: **David Lashway,** Partner Sidley Austin LLP

Lisa Monaco, Former U.S. Deputy Attorney General
Carsten Meywirth, Head of the Cybercrime Unit, Federal Criminal Police Office (BKA)
Sandra Joyce, Vice President Google Threat Intelligence Group
Edvardas Šileris, Head of Cybercrime Centre Europol, Netherlands
Dmitri Alperovitch, Co-Founder and Executive Chairman of Silverado Policy Accelerator

This panel focused on the evolving landscape of cybercrime and the increased collaboration required to address it. In particular, the panel reflected on how the relationship between cyber criminals and malicious state-affiliated actors has grown closer in the last ten years, with cyber criminality evolving into an efficient and profitable business model. The speakers stressed that these changes have made threats harder to counter and demanded closer collaboration between law enforcement and the private sector.

Carsten Meywirth pointed out the growth of cybercrime since 2015, noting how the lines between state-sponsored actors and cybercriminals had blurred. As a consequence, Lisa Monaco stressed that law enforcement needed to move beyond traditional methods and adopt a broader, more integrated approach. She highlighted the importance of being intelligence-led and threat-driven, focusing on prevention and disruption rather than simply investigating criminal activity after the fact. Sandra Joyce and Edvardas Šileris reinforced the idea that private sector collaboration was key in combating cyber threats and underlined the need for proactive intelligence sharing.

> Lisa Monaco:
> "Cybercrime, whether it's fueled by nation state actors or criminal groups, is a national security challenge and increasingly a public safety and economic security challenge."

Sandra Joyce added that such information sharing was only valuable if it translated into real action, warning that cybercrime was not only growing but also targeting vulnerable sectors like healthcare. She called on the private sector to act with greater urgency, moving from defense to more offensive strategies. Edvardas Šileris explained how Europol had sought to move beyond information exchange to actionable operations, though he cautioned that law enforcement still faced limits without lawful access to critical data. He stressed that without clearer agreements on data access, police risked being outpaced by increasingly sophisticated cybercriminals.

> Sandra Joyce:
> "Sharing intelligence is starting to be, in our community, the minimum viable thing that you could do."

Carsten Meywirth emphasized the need for international alliances, such as those fostered by Europol, and pointed to Operation "Endgame" – the largest European cyber takedown – as evidence that coordinated disruption could weaken criminal networks and strengthen the global response to cybercrime. Dmitri Alperovitch suggested a more aggressive, campaign-like approach to targeting cybercriminal organizations, drawing parallels to counterterrorism efforts. He argued that simply dismantling one group was not enough and called for more innovative and proactive tactics, such as sowing distrust within criminal ecosystems.

> Dmitri Alperovitch:
> "We have to be thinking about [cybersecurity] the same way we did in counterterrorism cases. The more you can inject chaos and distrust into that ecosystem, ... the more of an impact you will have on their operations in a very substantive and long-term way."

The panel concluded with a discussion on the importance of evolving international legal frameworks, such as the UN Cybercrime Convention, and the necessity of more agile and creative strategies to confront complex cyber threats. They emphasized that the challenge ahead lay in translating these frameworks and strategies into concrete action, ensuring law enforcement and partners could respond faster and with greater impact.

The three key takeaways were:

- **Turn sharing to action:** Intelligence exchange must translate into coordinated operations, that directly target adversaries and their infrastructure.
- **Confront infiltrations as hybrid threats:** The fusion of state and criminal actors requires strategies that bridge legal, technical, and policy domains.
- **Target infiltrations strategically:** Cybercriminal groups and state actors were described as reinforcing one another, requiring campaign-style approaches and international alliances to erode trust within these ecosystems.

TRANS-ATLANTIC VIEW

Moderator: **David Sanger,** White House and National Security Correspondent, The New York Times

Anne Neuberger, Former Deputy National Security Advisor for Cyber and Emerging Technologies at The White House

Sir Julian King, Former EU Commissioner

In the "Trans-Atlantic View" session, the experts explored the significance of cybersecurity cooperation and the current challenges that transatlantic cooperation was facing. The debate highlighted both areas of convergence – such as in the approach to securing critical infrastructure – and ongoing friction – namely how to safely develop AI – between the United States and Europe.

> Anne Neuberger:
> "Fundamentally, work on defense and on resilience is a precursor to any offensive operation."

The discussion opened with Anne Neuberger, who emphasized that building resilience in cyber defenses had to form the foundation of any credible strategy. If governments wanted to make it harder and more expensive for malicious cyber actors, they needed to be able to withstand blowback before engaging in offensive operations, she argued. Anne Neuberger also noted the increasing geopolitical competition in cyberspace and recalled how Russia's invasion of Ukraine had been preceded by a cyberattack on a satellite provider. Deterrence, she argued, depended on making operations riskier and costlier for adversaries while ensuring strong defenses. Offensive action, in her view, always had to be tied to clear objectives, whether tactical, signaling, or strategic.

> Sir Julian King:
> "A lot of the regulation – good or bad – is being done at the European level, so you need a European level to this discussion [of transatlantic cooperation]."

As the conversation continued, Sir Julian King reflected on the EU's significant strides in building cybersecurity resilience, arguing that early versions of the EU cybersecurity strategy had been inspired by the UK's experiences.While he noted that Europe had historically lagged on offensive capacities, the EU had invested heavily in regulation and defensive frameworks. While the United States followed a more hands-off approach regarding regulation, the transatlantic partners were more aligned than often perceived, Sir Julian King argued. For example, the U.S. regulatory approach to critical infrastructure was quite similar to the EU approach. The conversation also touched on the challenges of aligning regulatory approaches regarding new technologies, particularly artificial intelligence, with Anne Neuberger stressing the need for safe and transparent AI applications, especially in critical sectors like healthcare.

The key takeaways were:

- **Build defense before offense:** Cyber resilience was described as the essential foundation, ensuring the ability to withstand blowback before deploying offensive tools.
- **Bridge regulatory divides across the Atlantic:** The United States and the European Union are edging closer on the protection of critical infrastructure, yet their contrasting regulatory philosophies continue to shape different approaches.
- **Make AI the proving ground for cooperation:** Artificial intelligence was seen as the key test of transatlantic alignment, demanding safe, transparent, and responsible deployment in sensitive sectors.




SPOTLIGHT:

Risky Concentrations: Resilience on the Edge

Moderator: **Sasha O'Connell,** Senior Director for Cybersecurity Programs at The Aspen Institute

Claudia Plattner, President of the German Federal Office for Information Security (BSI)
Drew Bagley, Vice President and Counsel for Privacy and Cyber Policy at CrowdStrike
Pascal Andrei, Senior-Vice President Chief Security Officer at Airbus

This spotlight discussion shifted the focus from malicious actors to the fragility of the digital ecosystem itself. While much attention was paid earlier in the day on how to defend against malicious actors, this session debated the challenges of maintaining cybersecurity resilience in a world that increasingly depends on interconnected systems. Consolidation, interdependence, and hidden weak points were discussed as vulnerabilities affecting cyber resilience.

Drew Bagley stressed that resilience by design had to be the guiding principle in cybersecurity policies. He emphasized that organizations could not rely on one-size-fits-all approaches. Instead, resilience needed to be adaptive and continuously tested. Furthermore, Drew Bagley pointed to concentration risk as a growing blind spot in cyber policy. With this, he meant that companies should check components and supply chains, yet they often lacked a framework to assess the risk of an entire IT stack. He highlighted that such visibility gaps, especially in unmanaged devices, meant that threats could emerge unseen.

Pascal Andrei continued the conversation on the importance of visibility into IT stacks, by referencing Airbus's vast network of more than 18,000 suppliers, 1,000 of which were considered critical. He noted that in aerospace, security was inseparable from safety: any digital compromise could cascade into a physical risk. He described this as "safe-curity," insisting that only resilient-by-design approaches could protect both passengers and critical operations.

> Drew Bagley:
> "In any incident, one of the most important things is to stop the bleeding. You have to be focused on that while being transparent with stakeholders, and then having a single source of truth. If you don't have that single source of truth, then that's when you can have adversaries exploit that and take advantage."

> Pascal Andrei:
> "Having a business continuity plan all the time, is not only for concentration of risk but we also need to ensure that we have a clear vision of our critical assets."

> Claudia Plattner:
> "We have to sit down and get the basic maturity right. We are always talking resilience but we have to get the maturity right. ... Next time it won't be operational matter, it will be an attacker."

Claudia Plattner reflected on the lessons learned from the 2024 CrowdStrike service outage. Rules and standards already existed, she argued, but the failure lay in uneven implementation. For example, she highlighted that multiple parties, including vendors, partners, and governments, had overlooked basic responsibilities. She emphasized the need for forward-thinking improvements to strengthen cybersecurity resilience.

The panel concluded that technical solutions, while being critical, were not sufficient. True resilience required cultivating a culture of collaboration, transparency, and trust through implementation of existing rules, and coope-ration across governments, industries, and suppliers. Ultimately, the speakers agreed on the significance of preparedness, robust crisis management, and maintaining clear communication channels. The panelists finished arguing that only by sharing responsibility could future crises be managed effectively or, ideally, be prevented before they spread across the interconnected digital ecosystem.

The three key takeaways were:

- **Build resilience by design:** Cyber defenses must be adaptive, regularly tested, and address blind spots like unmanaged devices – from employee phones to IoT sensors, that often escape oversight but create hidden entry points for attackers.
- **Secure supply chains:** TEmbedding security clauses, demanding transparency, and conducting rigorous testing are essential to protect critical suppliers and operations.
- **Standards only work if applied:** The CrowdStrike outage showed that systemic failures in digital resilience came from uneven implementation, not from missing rules and frameworks.

GREETING BY STATE SECRETARY

Tobias Gotthardt

Bavarian Ministry of Economic Affairs

The evening greeting by State Secretary Tobias Gotthardt was characterized by a mix of urgency and optimism. He remarked that the Munich Cyber Security Conference and the Munich Security Network had firmly established Munich as a global cybersecurity hub, bringing together experts from across sectors. The State Secretary acknowledged the achievements of the organizers, noting that such platforms had become indispensable in uncertain times.

He warned that cyberattacks were growing not only in number but also in speed and sophistication. Actions that once took weeks, he said, could now be carried out in hours, from stealing sensitive data to paralyzing entire systems. Citing a Bitkom study, he pointed out that Germany had suffered an estimated 266 billion EUR in economic damage from cyber incidents in the past year alone.

Tobias Gotthardt argued that resilience could only be achieved through collaboration across business, politics, and civil society. He praised the Bavarian Ministry of Economic Affairs for its proactive approach to cybersecurity and investment in a high-tech agenda, and welcomed EU progress through the Cyber Resilience Act and new initiatives such as the Cybersecurity Skills Academy. Finally, he stressed the value of the MCSC for SMEs, which gained vital opportunities to network, learn, and strengthen their defenses. These closing remarks of the first day of the MCSC 2025 conference expressed the desire to find the best practices to address the rising uncertainty in cyberspace.

> Tobias Gotthardt:
> "It is imperative that all of us continue to work together to provide robust protection in cyber space."

TECHNOLOGY MATTERS:

AI, Quantum Computing, Promising Perspectives

Moderator: **Gabriel Mitschke-Collande,** Chief Digital Officer at Giesecke+Devrient

Gerhard Fettweis, Vodafone Chair Professor at Technical University Dresden

Michele Mosca, Co-Founder and Professor at the Institute for Quantum Computing at University of Waterloo

Jacky Fox, Global Cyber Security Strategy Practice Lead, Accenture

Thomas Saueressig, Board Member of SAP

Eva Maydellh, Member of the European Parliament

To launch the second day of the conference, the first panel explored the profound impact that AI and quantum computing will have on industry, society, and security. The discussion re-flected both excitement and unease: while innovation was accelerating, it was noted that gov-ernance and preparedness lagged behind, leading to greater uncertainty for the future.

Jacky Fox kicked off the discussion by warning that AI-driven threats such as deepfakes were becoming more sophisticated, while only a third of organizations had put safeguards in place. She mentioned that fraud chains were already being transformed by AI, but many firms still treated risks as hypothetical. On quantum computing, Jacky Fox noted that too few compa-nies were auditing their cryptographic systems, often assuming a "non-event" scenario – simi-lar to the overhyped concern about Y2K – that would leave them dangerously exposed once quantum code-breaking arrived. Michele Mosca underscored her warning. After decades of gradual advancement, he anticipated more breakthroughs with the potential to transform en-tire industries in the years ahead. His implication was clear: resilient cryptographic infrastruc-ture had to be built immediately, not later.

> Jacky Fox:
> "AI and quantum are areas where the knowledge, unfortunately, is pretty limited. ... This worries me, because I believe we can take the wrong decisions today –in terms of policies that would impact the future – simply because we are unable to propel ourselves and see how those technologies will impact our societies."

The panel subsequently discussed the crucial role of policy makers in addressing emerging threats. MEP Eva Maydell drew attention to the challenge for policy makers of regulating fast-moving technological advances while grasping their broader implications. She stressed the need for the EU to adjust its regulatory approach to foster innovation while ensuring societal safety. While the EU had made progress, such as through the 2023-2024 Horizon Europe Dig-ital, Industry, and Space funding, Eva Maydell cautioned that without a coherent strategy and stronger industry adoption, the EU risked falling further behind. Industry voices echoed her concerns. Thomas Saueressig echoed this sentiment, stressing that the EU's slower adoption of cloud and AI was holding it back economically. Gerhard Fettweis highlighted the potential for AI-powered robotics, ranging from consumer products to autonomous driving. He also noted that the EU could draw on its leadership in sensors and supply chains, but only if it act-ed decisively.

> Eva Maydell:
> "There's been such a big public outlash against the numerous legislative files that are that are out there. I think, particularly when it comes to cybersecurity... we've tracked them down to around 16 pieces of legislation."

> Gerhard Fettweis:
> "Things have changed less in terms of technology and more in terms of awareness."

The panel concluded with a clear call: the EU cannot afford hesitation. Securing a competitive role and greater clarity on what comes next in the AI and quantum era required immediate investment in AI and quantum technologies, agile regulation, and a focus on strengthening resilience.

Three key takeaways from this session included:

- **AI and quantum demand urgent preparedness:** Both technologies are advancing faster than governance, exposing gaps in resilience, cryptography, and organizational standards.
- **Policy and vision are lagging:** A persistent knowledge gap among policy makers risks leaving regulation reactive rather than enabling.

› **The EU risks losing ground:** Without a coherent strategy and faster adoption, the EU may fall behind global competitors already scaling these technologies, unless it leverages its industrial strengths in sensors, supply chains, and robotics.

FOCUS INDIA:

Cyber Resilience Agenda 2025

Moderator: **Ralf Wintergerst,** Global President of Bitkom, Group CEO of Giesecke+Devrient

Nandan Nilekani, Co-Founder and Chairman of Infosys Limited, India

In the "Focus India" session, the speakers explored how technology has transformed the world's largest democracy and considered its future trajectory.

Nandan Nilekani, co-founder of Infosys and a central figure in India's digital revolution, shared critical insights into the evolution of India's digital infrastructure, particularly in the areas of digital identity and payment systems. He argued that in an increasingly volatile world, governments, companies, and citizens needed to learn to navigate uncertainty rather than lament it, a mindset that had enabled India to adapt and progress forward.

> Nandan Nilekani:
> "I firmly believe that India will be the AI use capital of the world."

Nandan Nilekani recounted his role in developing Aadhaar, India's national digital ID system, which today gives more than 1.3 billion people access to vital services and is authenticated around 80 million times each day. Coupled with mass mobile penetration and the UPI payments platform, now processing 17 billion transactions monthly, he explained that this infrastructure had transformed financial inclusion, making India a prime example of

how technology can scale to meet the needs of a vast population. Nandan Nilekani emphasized that privacy was built into the system from the start, with minimalistic system design and data empowerment ensuring that control lay with individuals rather than aggregators.

Looking ahead, Nandan Nilekani predicted that India would become the "AI use capital of the world." With 22 official languages, he explained that linguistic data resources were being built in India to make AI more accessible and practical for all. He also mentioned that AI's potential in areas like agriculture and education would drive real-world improvements for millions. He concluded his remarks by discussing his philanthropic focus on education and his efforts to design future energy grids with a vision for a unified protocol to enable a global energy transition.

His remarks lead to the following key takeaways:

- **Digital transformation at scale:** India's ID and UPI systems have delivered financial inclusion and created a unified national digital market.
- **Privacy by design:** Minimalist architectures and user-controlled data have been central to building trust and resilience.
- **AI as the next frontier:** India aims to lead in applied AI, using its linguistic diversity to make technology accessible and to unlock realworld benefits in agriculture, education, and beyond.

CYBER DEFENSE IN 2025

Moderator: **Andrea Rigoni,** Global Health and Public Sector Group Lead at Accenture

LtGen Michael Vetter, Director General Cyber and Information Technology Division and CIO, German Ministry of Defence

Hannah Neumann, Member of the European Parliament, Group of the Greens/ European Free Alliance

Carl-Oskar Bohlin, Swedish Minister for Civil Defence

MajGen Zac Stenning, Director of Strategy and Assistant Chief at UK Strategic Command

Chris Inglis, Former National Cyber Director at The White House, USA

The panel on Cyber Defense in 2025 painted a sobering picture of a world where the boundaries between peace, crisis, and war are increasingly blurred, and where resilience demands a whole-of-society effort.

Andrea Rigoni set the stage by recalling NATO's efforts to establish cyberspace as the fifth operational domain for defense. He stated that unlike land, air, sea, or space, cyberspace lacked the laws of physics, which made it far more difficult to establish clear rules and strategies. In this domain, private companies, governments, and citizens were equally exposed, all reduced to the same vulnerability of an IP address, he argued.

LtGen Michael Vetter emphasized that agility and flexibility were central to future defense strategies, advocating for a "whole-of-society" approach that involved military, government, and private sectors to strengthen resilience. He also underscored that Germany had made significant progress in cyber defense but still needed to improve coordination between military and civilian structures.

Hannah Neumann highlighted the growing scale of cyberattacks carried out by hostile states and organized criminal groups. Preparedness, she argued, had to begin at the individual level: just as society had learned new habits during the pandemic, digital hygiene also needed to become second nature. But regulations, she warned, remained fragmented, with overlapping authorities leaving responsibilities unclear. Europe needed clarity,

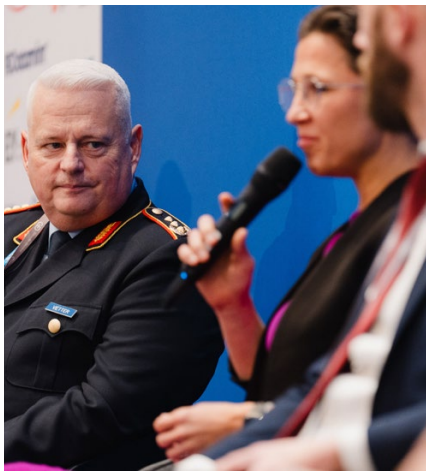
governance, and above all, greater sovereignty in managing data and infrastructure rather than relying so heavily on the United States.

Carl-Oskar Bohlin explained how Sweden was reviving its Cold War-era "total defense" concept, integrating cyber as a core pillar. He noted that Sweden's new national cybersecurity center mobilized military and civilian capacities side by side, including the use of conscripts to safeguard privately owned critical infrastructure. MajGen Zac Stenning then raised concerns about the scope of cyberattacks, which had increased from 430 major incidents to 90,000 attacks on British military networks within a year. To meet this challenge, he argued for a multi-layered defense strategy with partnerships in industry and academia, expanding on the traditional joint military approaches.

Finally, Chris Inglis urged a mindset shift: defense, not offense, had to be the priority in cyberspace. Drawing on lessons from Ukraine's resilience, he argued for segmentation, backups, and coalition-building. The key, he concluded, was to make cyberattacks costly for adversaries and to raise the baseline of digital literacy across society.

The key takeaways were:

- **Blurred lines of conflict:** In contrast to other NATO defense domains, cyberspace has no "laws of physics" to provide fixed rules. With the lines between peace, crisis, and war increasingly blurred, this has produced a destabilizing environment that leaves governments, businesses, and citizens equally vulnerable.
- **Whole of society approach:** Effective cyber resilience requires more than military strength. It depends on civilian preparedness, regulatory clarity, and coordinated action across governments, industries, and international partners.
- **Defense as priority:** Cyberspace can be made defendable through layered protections, backups, and coalitions, but only if societies raise digital literacy and ensure that launching attacks become more costly than deterring them.



PREPAREDNESS AND RESILIENCE IN 2025:

What to Take Out from the Niinistö Security Report?

Moderator: **Oliver Rolofs,** Co-Founder of MCSC & Founder and Managing Partner of Commvisory

Despina Spanou, Principal Adviser, DG CNECT, European Commission
Rolf Schumann, Co-CEO of Schwarz Digits, Germany
Volodymyr Lutchenko, CTO, Kyivstar

In October 2024, the European Commission published the report, "Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness," by Special Advisor Sauli Niinistö, which provided recommendations for the EU to strengthen its preparedness. The report set the stage for a discussion that combined lessons from building cyber resilience in wartime Ukraine with recommendations for strengthening EU preparedness amid growing geopolitical uncertainty.

In his opening remarks, Volodymyr Lutchenko shared firsthand experience of sustaining a nationwide telecom system in wartime conditions. He explained that damage to data centers or transport hubs, though serious, could be managed, whereas the shortage of skilled personnel posed a longterm vulnerability. His principal advice to the EU was to act swiftly by conducting infrastructure audits and cybersecurity readiness checks to address vulnerabilities before they escalate during a crisis.

This proactive approach aligned with Despina Spanou's call for a more integrated, multi-sector strategy to cybersecurity, drawing inspiration from military models of cooperation. She pointed out the importance of enhancing crisis coordination frameworks and investing in informationsharing hubs to improve the overall security posture across Europe.

Rolf Schumann brought in the private sector perspective, stressing that companies could not afford to wait for government action. Using Germany's reliance on critical digital infrastructure as an example, he underlined the importance of digital sovereignty in enabling businesses to adequately protect their systems.

Ultimately, the panel emphasized that only continuous cooperation between the public and private sectors could provide an effective defense against malicious cyber actors. They also highlighted the importance of forward-looking strategies such as "pre-bunking" disinformation and ensuring that strong cybersecurity measures are implemented consistently across industries and nations.

The key takeaways from this session were:

- **Building resilience starts with people:** Ukraine's experience shows that infrastructure can be restored, but a shortage of skilled cybersecurity professionals remains the real vulnerability. The Niinistö Report urges Europe to act now with audits, readiness checks, and investment in human capacity.
- **Preparedness requires integrated coordination:** Military-style coordination and shared information hubs are key to Europe's ability to handle cyber crises before they escalate.
- **Security is a shared responsibility:** Governments set the framework and provide coordination, but businesses must not wait on regulation alone. Europe's digital sovereignty depends on companies and public actors moving in tandem, each taking proactive steps to secure critical systems.

VANTAGE POINT

Audrey Tang

Cyber Ambassador, former Minister of Digital Affairs, Taiwan

The conference continued with a powerful keynote from Audrey Tang, highlighting Taiwan's role on the frontlines of defending democracy against sophisticated cyber threats and explaining how Taiwan has managed to find some clarity amid geopolitical and technical uncertainty.

She explained that Taiwan repeatedly faced surges of state-backed cyberattacks whenever high-profile political events attracted global attention. She explained that during visits from senior U.S. officials – such as when U.S. Speaker of the House Nancy Pelosi visited in 2022 – denial-of-service traffic spiked sharply, which put Taiwan into several days of heightened alert each time. As a consequence, the Ministry of Digital Affairs had adopted a rapid-response posture, built on zero-trust cybersecurity architecture, agile workflows, and pre-bunking campaigns that contained damage before it spread.

She also highlighted the vulnerability of physical infrastructure, citing repeated severing of subsea cables to outlying islands and the widespread disruption caused by a major earthquake that cut power and destroyed roads. In response to such incidents, she explained, Taiwan in-vested in microwave relays, satellite backups, and mobile 5G base stations airlifted into disas-ter zones – measures that kept communities online and first responders connected when con-ventional systems failed. Her argument was that cyber resilience cannot be separated from physical resilience.

> Audrey Tang:
>
> "No democracy is an island – not even Taiwan – and we deeply value ongoing international partnerships, in forums such as this one, as well as multilateral exercises."

Audrey Tang further addressed emerging risks such as deepfakes and information manipula-tion and outlined Taiwan's democratic innovations, from SMS polls and large-scale citizen assemblies to AI-assisted deliberation, that had helped craft consensus. This process also led to new legislation requiring tech platforms to verify ads, hold liability for scams, and ensure accountability, she noted. At the same time, she explained that Taiwan had piloted "pro-social media," a model designed to surface shared values and encourage constructive public dialogue rather than amplify polarization.

She concluded by stressing that Taiwan could not carry this burden alone. She offered that its recurring cyber defense exercises across critical sectors, from healthcare to water supply, were open to international partners for joint training, intelligence sharing, and co-development of defenses. Her closing message was clear: securing democracies in the digital age demands transparency, innovation, and collective action.

The three key takeaways from the keynote were:

- **Taiwan on the cyber frontlines:** As a democracy under constant state-backed attacks, Taiwan has become a central actor in cybersecurity, adopting zero-trust systems, rapid workflows, and pre-bunking campaigns to turn politically timed disruptions into manageable events.
- **Cybersecurity needs physical backups:** Cable cuts and earthquakes revealed how quickly connectivity could collapse, underscoring the need for redundant systems such as satellite links, microwave relays, and mobile 5G stations to keep communities online.
- **Democracy as defense:** Taiwan pioneered democratic innovations, citizen assemblies, and AI-assisted deliberation, that turned public input into concrete laws holding platforms accountable and promoting "pro-social media" spaces for constructive debate.

THREE QUESTIONS FOR

Moderator: **Stormy-Annika Mildner,** Executive Director Aspen Institute Germany

Hanno Pevkur, Minister of Defence of the Republic of Estonia

The following session added clarity to Europe's current security situation. Hanno Pevkur delivered an urgent message about the security challenges facing Europe. He stressed that Estonia had to coexist with Russia, a neighbor that had systematically employed hybrid warfare, cyberattacks, and political manipulation. He warned that Moscow could test NATO without resorting to full-scale war, as even small provocations may erode collective defense. Pointing to Russia's 2007 cyberattacks on Estonia as a turning point, he argued that any vulnerability within NATO could invite further destabilization, making unity and resolve from the West indispensable.

> Hanno Pevkur:
> "To invest 5% today during peace time for defense is still much less to spend than 25% or 30% of your GDP during wartime."

Building on this, Hanno Pevkur also addressed the political challenges within Europe and argued that defense spending and the commitment to a collective defense strategy should be central to political discourse. Investing five percent of GDP in defense during peacetime was, he said, still far cheaper than financing a war consuming 25 to 30 percent of GDP. The true danger, he suggested, lay in complacency, especially in parts of Europe more distant from Russia's borders.

Despite this sobering outlook, Hanno Pevkur closed on a cautiously optimistic note. Drawing on Estonia's own history of resilience, he argued that even smaller nations, with unity and determination, could withstand the most formidable threats. What mattered most was clear leadership, honesty with citizens, and a shared commitment to collective defense.

The three main takeaways from this session were:

- **A new era of confrontation:** Cyberattacks and hybrid provocations have become Russia's way of testing NATO, threatening to further destabilize its unity and collective defense.
- **Defense requires honesty:** Investment in defense must be part of public discourse not only in wartime but especially in peacetime, making threats visible and tangible for citizens and underscoring that beyond money, security depends on honesty.
- **Unity is the decisive weapon:** Estonia's own history showed that even small nations could resist larger powers if they acted with resolve, but complacency in parts of Europe risked undermining the collective defense that all depend on.

Information Ecosystems in a Changing World

Moderator: **Vivian Schiller,** VP and Executive Director at The Aspen Digital

Lisa Kaplan, Founder & CEO, Alethea
Ginny Badanes, General Manager of Democracy Forward at Microsoft
Maia Mazurkiewicz, CEO of PZU Foundation & Co-Founder of Alliance4Europe
Nicola Hudson, Partner and Cybersecurity, Data & Privacy Global Lead at Brunswick Group
Vilas S. Dhar, Patrick J. McGovern Foundation

The panel began by confronting an uncomfortable reality: The foundations of trusted information, the panelists warned, were steadily eroding. Independent news outlets were in decline, major platforms had reduced their content moderation efforts, and artificial intelligence had added new layers of complexity to already fragile systems. These vulnerabilities had become particularly visible in 2024, a year marked by an unusually crowded election calendar, the panelists argued.

Ginny Badanes opened the discussion by describing how state-backed actors had adapted AI for subtle but effective influence operations. She noted that Russia had experimented with deepfake audio clips, inserting them into real campaign footage in ways that were hard to detect with the naked eye. She then shared that Iran had created more than a hundred fake news outlets using generative AI to mass-produce manipulated content, blending propaganda into seemingly reliable sources. She expressed that while the impact was hard to measure, the technology itself presented a new level of sophistication in misinformation campaigns.

> Ginny Badanes
> "There need to be technology solutions, there needs to be public policy, there needs to be societal resilience and education efforts."

Maia Mazurkiewicz continued the conversation but cautioned against framing AI itself as the threat. Like a double-edged sword, she highlighted that it could be used constructively or destructively. She cited Romania, where elections were annulled after evidence of manipulation. She further highlighted that during the election campaign in Germany, narratives had emerged around migration that demonstrated how easily extremist messages could be amplified.

Turing to the private sector, Nicola Hudson expanded on the broader implications for businesses, noting that AI-driven misinformation could harm corporate reputation, making it essential for businesses to be proactive in managing these risks. She explained that deepfake audio scams had already cost millions, while companies faced reputational attacks they were ill-prepared to counter in real time. Lisa Kaplan added that corporations were increasingly swept into geopolitics, with brands drawn into synthetic conspiracies or being directly targeted by governments.

> Nicola Hudson:
> "It [the responsibility] can't just sit with the CISO and the poor 20-year-old who's doing a bit of monitoring. It has to be an all-business kind of approach."

Looking ahead, Vilas S. Dhar introduced the concept of AI-based belief arbitrage. He warned that AI could systematically map cognitive biases and nudge individuals step by step from mainstream to extreme positions. Such campaigns, automated and personalized at scale, would not even violate current laws or regulatory frameworks, he remarked.

The panel concluded with a call for a comprehensive, society-wide response to these challenges, focusing on education, collaboration, and policy development to safeguard against the manipulation of information on a global scale. They argued for a renewed social contract for the information age, anchored in transparency, shared responsibility, and resilience.

> Vilas S. Dhar:
> "The fundamental challenge is that we continue to believe that misinformation or disinformation are the real challenge and we come up with structures that respond to that – from pre-bunking to watermarking to figuring out the ways that we can address deep fakes. There's a more fundamental challenge that AI enables, in a way that we've never really seen before, which is the use of independently credentialed and verifiable information that's used for the manipulation of an information ecosystem."

The three key takeaways were:

- **AI escalates disinformation tactics:** Deepfake audio and AI-generated fake news sites show how state actors like Russia and Iran can manipulate information at scale, making disinformation harder to detect and more sophisticated.
- **Vulnerabilities extend beyond politics:** Misinformation now targets businesses and individuals, with deepfake scams costing millions and corporations being dragged into geopolitical narratives they are unprepared to counter.
- **From disinformation to belief manipulation:** Emerging risks go beyond fake content. AI can exploit cognitive biases to gradually shift individuals toward extreme views, a threat still largely unregulated and requiring urgent, society-wide safeguards.





KEYNOTE

Henna Vikkunen

Executive Vice-President of the European Commission

Henna Vikkunen opened her keynote with a clear statement: cybersecurity was no longer a technical niche but the backbone of Europe's resilience, economic security, and defense. Recent incidents targeting critical infrastructure such as energy grids, healthcare facilities, and subsea cables demonstrated how digital attacks carried real-world consequences.

Yet, while threats had become interconnected, Henna Vikkunen argued that responses remained fragmented. Too often, she stated, governments, businesses, and international organizations worked in isolation. She called for breaking down these barriers through stronger information-sharing, public-private partnerships, and military-civil cooperation. Only a whole-of-society approach, she stressed, could secure the EU against systemic risks.

Looking ahead, she warned that the geopolitical turbulence of 2025 would fuel further cyber operations, making global governance an urgent priority. Enhanced cooperation between the EU and NATO was essential, she argued, alongside comprehensive preparedness for worst-case scenarios. She explained that the EU's new Cybersecurity Reserve, AI-enabled detection systems, and sector-specific action plans, such as for healthcare, were designed to strengthen capacity and offer rapid support in crises.

Henna Vikkunen also discussed the role of emerging technologies in both cybersecurity and digital sovereignty and announced the development of a cybersecurity roadmap to map EU dependencies and strengths, direct strategic investments, and bolster Europe's industrial base. Lastly, she highlighted efforts to simplify regulations and reduce red tape, while ensuring the EU's sovereignty in cybersecurity by strengthening its industrial policy.

For Henna Virkkunen, the task was urgent and collective: Europe's security depended on preparedness, innovation, and unity across borders and sectors.

> Henna Vikkunen:
>
> "Cybersecurity is no longer a niche technical issue. It's very much the key for our resilience when we speak about our societies, but also it's very critical for our economic security, and of course for all our defense."

The three key takeaways from the keynote were:

- **Cybersecurity is the backbone of resilience:** Attacks on energy, healthcare, and subsea cables show that digital threats carry real-world consequences and must be treated as central to Europe's defense.
- **The threat of fragmentation:** Fragmented responses leave Europe exposed; resilience requires EU-NATO cooperation, rapid support tools like the Cybersecurity Reserve, and sector-specific preparedness plans.
- **Roadmap to digital sovereignty:** A new EU cybersecurity roadmap, together with the Cyber Resilience Act, will map dependencies, guide strategic investments, simplify regulation, and strengthen Europe's industrial base to secure digital sovereignty.

Security Sovereignty by Regulation?

Moderator: **Alexander Evans,** Associate Dean, London School of Economics

Dennis-Kenji Kipker, Research Director at Cyber Intelligence Institute
Axel Deininger, President of ECSO & CEO of secunet
Hans de Vries, Chief Cybersecurity and Operations Officer at ENISA
Thomas Rosteck, Division President for CSS at Infineon Technologies
Jason Ruger, CISO at Lenovo

The final panel of the MCSC main-track took on one of the most contentious questions in cy-bersecurity today: can regulation strengthen sovereignty without stifling innovation? The dis-cussion was shaped by a clear contrast: while private companies treat regulation as a perma-nent board-level issue, governments tend to approach it sporadically, often in reaction to cri-ses. With states advancing regulatory diplomacy abroad and the EU crafting an increasingly complex legal framework, the panel explored both the potential and the challenges of govern-ing digital security through regulation.

Dennis-Kenji Kipker argued that the debate should no longer focus solely on cybersecurity, but on digital resilience in a world of hybrid threats. Pointing to the COVID-19 pandemic and Russia's war in Ukraine, he stressed that legislative responses had consistently lagged behind the fast-evolving cybersecurity landscape. Axel Deininger concurred on the need for regula-tion but cautioned that the EU's fragmented approach undermined its effectiveness. With each member state crafting its own rules, he noted, small and mid-sized companies in particu-lar faced an unmanageable patchwork. Harmonization and simplification, he emphasized, were essential if regulation is to enable security rather than delay it.

Hans de Vries pointed to IoT devices as a case study of why regulation mattered: insecure by default, they had become massive attack vectors. The EU's NIS2 Directive and Cyber Resili-ence Act had set global benchmarks, but alignment and consistent implementation across bor-ders remained the key challenge.

> Hans de Vries:
> "We can be proud that we do have the most advanced and holistic legal framework in the world, when you look at the NIS2 and the Cyber Resilience Act that follows."

From the corporate perspective, Thomas Rosteck and Jason Ruger underscored the role of industry in strengthening cybersecurity. Thomas Rosteck insisted that regulation was indis-pensable because market dynamics alone would not secure products: security was not a fea-ture customers demanded. He urged regulators to set limitations without prescribing technical solutions, leaving room for innovation. Jason Ruger echoed the call for dialogue, noting that multinational corporations operating in 150 countries faced not just EU fragmentation but global inconsistencies. He argued for greater engagement between governments and industry to ensure rules were practical and enforceable.

> Thomas Rosteck:
> "Regulation is hindering innovation, and that might be true in some instances. So that's why I think regulation should tell me what you expect me to do, not how I do it, because technology will change over time."

> Jason Ruger:
> "Regulation should try to be preventative."

Throughout the discussion, the panelists circled back to a common theme: regulation had to be more than a compliance exercise. Regulation needed to enable trust, reduce the EU's depend-ence on foreign technology, allow for the mutual recognition of standards, and make resilience scalable across borders and sectors, they argued. The discussion served as a strong conclusion to the conference: regulation is a key part of strengthening digital sovereignty and creating clarity in an uncertain cyberspace.

The three key takeaways were:

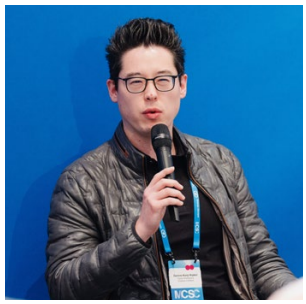
- **Breaking the maze of rules:** Europe's fragmented national implementations of cybersecurity laws risks undermining resilience. Harmonization and simplification are essential for regulation to enable, rather than hinder, security.
- **Good Regulation is necessity for innovation:** Market forces alone cannot deliver secure products. Regulation has to set clear expectations, especially in areas like IoT, while still leaving space for innovation.

› **Dialogue for rules:** Multinational companies face not only EU fragmentation but also global inconsistencies. Effective regulation requires constant exchange between governments and industry to ensure practicality, enforceability, and trust across borders.










CLOSING WORDS

Claudia Eckert

Chairwoman Security Network Munich

In her closing remarks, Claudia Eckert distilled the key lessons of the 2025 MCSC. She stressed the urgency of accelerating efforts, advocated leveraging AI to narrow the gap between attackers and defenders, and called for a shift toward more proactive, offensive defense. She emphasized the need to simplify and harmonize regulations, to fully harness technology in preparation for future challenges, and to invest in emerging fields such as AI and robotics. Eckert also underscored the importance of broad-based education to enable citizens to contribute to cyber defense, and urged innovative thinking to disrupt attackers' business models and raise the costs of their operations. She concluded that the conference had provided crucial clarity on how to strengthen cybersecurity in a time of growing geopolitical uncertainty. Her message was clear: Europe's security will depend on urgency, innovation, and collaboration.

DEF CON Meets MCSC: Security Talks in Cooperation with DEF CON

OPENING REMARKS

Jeff Moss
President and Founder of DEF CON

In his opening remarks, Jeff Moss traced the evolution of DEF CON, one of the world's largest hacker and information security conferences. While it began as a gathering focused exclusively on hackers, over time it grew into a broader infosec conference. In recent years, he noted, DEF CON had benefitted greatly from integrating government partners, underscoring the importance of stronger information exchange between technical experts and policymakers. Against this backdrop, Moss explained that the following discussions aimed to bring some of the DEF CON spirit to the MCSC for the first time – contributing to the conference's overarching goal of providing clarity in a field marked by profound uncertainty.

FIRST PANEL:

AI, Automated Attack & Defense

Moderator: **Jeff Moss,** President and Founder of DEF CON

Perri Adams, Special Assistant to the Director of DARPA
David Weston, Vice President, Enterprise and OS Security at Microsoft
Yan Shoshitaishvili, Assistant Professor at Arizona State University

The crossover between DEF CON and the Munich Cyber Security Conference offered a rare fusion of worlds: the freewheeling spirit of the hacker community meeting the structured setting of policy makers and industry leaders. Moderator Jeff Moss reminded the audience that DEF CON had always thrived on curiosity and discovery, free from commercial agendas or career incentives. By bringing that ethos to Munich, he suggested that participants could glimpse cybersecurity's future through the eyes of those who had long anticipated problems others only later recognized. That spirit of foresight and experimentation set the stage for a candid discussion on how artificial intelligence was reshaping both cyberattacks and defenses.

> Jeff Moss:
> "AI ... continues to be very good at aiding human analysts and doing small tasks, like munching through logs. It continues to be, in my opinion, underwhelming and oversold at replacing humans."

David Weston opened the discussion by noting how cyberattacks had professionalized at unprecedented speed with the advent of AI. He explained that both criminal groups and nation-state actors had adapted more quickly than defenders, underscoring the continued importance of secure software practices. Fundamentals such as minimizing flaws, he argued, remained essential despite rapid technological change. At the same time, Weston cautioned that certain legacy protections – such as Address Space Layout Randomization (ASLR), which random-izes memory locations of key system components – could slow performance without signifi-cantly deterring attackers. Instead, he advocated deterministic approaches, memory-safe programming languages, and formal verification as more effective ways to keep pace with adversaries.

> David Weston:
> "We're seeing many more capable cyber criminals in terms of their ability to build tools fast and adapt. One of the things I see quite frequently is ... attackers are able to move from a disrupted state – where we've broken their tools and techniques – into research and development. They move much faster than I've seen in the past."

While Yan Shoshitaishvili agreed mostly with David Weston, he also noted that lone hackers could no longer thrive against hardened systems. Complex attacks required teams, advanced tooling, and months of preparation, he explained. While AI proved useful at identifying vulnerabilities, he noted that it still fell short at reliably exploiting them, keeping human expertise central to offensive operations.

> Yan Shoshitaishvili:
> "As hardware gets more and more complicated, more and more optimized, these optimizations lead to kind of shortcuts that can be exploited by hackers."

Perri Adams stressed that automation had long been embedded in cyber operations. AI, she argued, was best seen as a force multiplier in this existing ecosystem. Yet, its limits were clear to her: without sufficient data, AI struggled with novel vulnerabilities. Still, Perri Adams pointed to emerging opportunities in automated vulnerability discovery, patch generation, and scalable defense, especially as software supply chain attacks became the weapon of choice for adversaries.

> Perri Adams:
> "I talked about all the automation that we'd seen up until this point and there were a lot of gaps that weren't covered by automation that was driven by algorithmic or logical programming. And so AI can really fit into uh those gaps."

The panelists agreed that AI would not supplant human defenders, but that it would determine whether societies are able to keep up in a world where speed and automation define survival.

The three takeaways from this session were:

- **Cyberattacks outpace defenses:** Professionalized attackers adapt faster than defenders, making memory-safe coding and formal verification essential to close the gap.
- **AI as force multiplier, not replacement:** AI enhances automation and speeds up vulnerability discovery and patching but remains limited without sufficient data and still depends on human expertise.
- **Future of resilience hinges on speed:** EIn a world where supply chain attacks dominate and automation defines survival, societies must invest in scalable defenses to keep pace.


SECOND PANEL:

Super Empowered Individuals, Private Sanctions, Conflicted Parties, Defend Forward

Moderator: **Jeff Moss,** President and Founder of DEF CON

Linus Neumann, Chaos Computer Club
Joel Krooswyk, Federal CTO at GitLab

The following session explored how power, responsibility, and governance were shifting in cyberspace. The stage was set by explaining the idea of Super Empowered Individuals (SEIs) – actors whose control over critical technologies granted them geopolitical leverage. The panel recalled that in the past, a single engineer's choice of DNS settings could affect billions of users worldwide. This level of control, they argued, underscored concerns about the influence of private actors, especially when companies acted on their own initiative and risked circumventing government regulation or sanctions. The discussion therefore turned to a central issue: in an era where cyberspace

is ever more entangled with geopolitics, do corporations assume a political role?

The ethical dilemmas around SEIs also included the role of open-source software. Joel Krooswyk of GitLab described the growing pressure to scrutinize contributions from regions seen as hostile, especially China, even as open-source software underpinned 90 percent of global software. Linus Neumann of the Chaos Computer Club cautioned against fragmenting the shared ecosystem into competing "splinternets," stressing that openness has long been one of the internet's greatest strengths. At the same time, he and others acknowledged the risks, pointing to recent supply-chain backdoors such as the attempted compromise of the XZ compression library, in which malicious code had been embedded into widely used data compression software affecting Linux distributions.

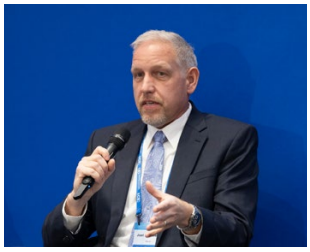
> Joel Krooswyk:
> "When you're talking about source code, how critical is it? It's your backbone, right? So you have to very carefully watch where your contributions are coming from."

> Linus Neumann:
> "I would like to remind us of the success story of open-source software in bringing advance to societies worldwide and creating a multinational community beyond all these conflicts and the interests of states and large corporations. ... It is a valuable idea to uphold."

From there, the discussion circled back to accountability and liability: when open-source code was weaponized, or when corporations enforce private sanctions, who bore responsibility? The panelists argued that software curators were being created to create some accountability within the open-source software, but ultimately, no agreement was made on who bore final accountability. With civil society often unprepared for state interference, the panelists urged more transparent standards, curated safe repositories, and new forms of governance to protect both innovation and trust.

The three key takeaways were:

- **Private sanctions shift power:** Tech companies now act as geopolitical actors, cutting off access and enforcing norms without state oversight.
- **Open-source under pressure:** While vital to global software, open-source software faces rising risks from malicious contributions and geopolitical fragmentation.
- **Neutrality is eroding:** In a conflict-driven digital landscape, no major provider remains unaffected, making accountability and shared safeguards essential.



CLOSING PANEL:

All Hands on Deck, Capacity Building, The Next Generation

Moderator: **Phil Stupak,** Former Assistant National Cyber Director at The White House

Jake Braun, Executive Director of the Cyber Policy Initiative, University of Chicago
Chris Painter, Former President of the Global Forum on Cyber Expertise Foundation
Carole House, Former Special Advisor for Cybersecurity at NSC, USA

The final discussion of the conference brought DEF CON's hacker ethos into dialogue with policy makers and industry leaders, underlining a shared challenge: capacity building for the next generation of cybersecurity. The tone was set by noting that technical skills, sustainable frameworks, and civic engagement could determine whether societies could withstand escalating digital threats.

Chris Painter reminded the audience that capacity building was not just about transferring resources, but about ensuring that countries were capable of responding to cyber threats themselves. He underscored that mutual support had created a safer global cyber ecosystem, where transnational cooperation was essential. Many countries still lacked strategies, laws, and/or institutions, leaving them dependent on external support, he noted. Mutual security, he also stressed, depended on helping others close their weakest links.

> Chris Painter:
> "Capacity building is foundational to everything else."

Carole House drew on her White House and U.S. Treasury Department experience to highlight the transnational nature of cybercrime, which often stretched across multiple jurisdictions and infrastructures. She urged a demand-driven approach: projects had to meet countries' actual needs rather than replicate off-the-shelf templates to achieve progress on capacity building. She further cited programs like the FALCON Initiative, which deployed experts to assist Costa Rica during a ransomware crisis, and showed how direct and targeted capacity building could deliver real impact.

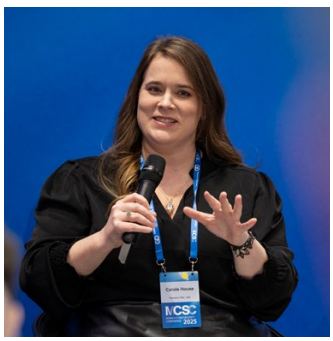
> Carole House:
> "So any kind of capacity building must be transnational, and also has to be public and private, because industry is often the target."

Jake Braun shifted the focus of the discussion to the cyber workforce gap. He shared his experience in cyber policy, explaining the importance of defining cyber jobs and creating a structured workforce to address gaps in the sector. He also highlighted the need for creative solutions and greater civic engagement, exemplified by initiatives like the Hacker's Almanac, which leveraged volunteer expertise to support critical infrastructure.

> Jake Braun:
> "What governments across the world are doing right now isn't solving the problem [of ransomeware]. So, we have to do something else, something more beyond what we're doing today."

The three key takeaways were:

- **Capacity building is security:** Building national strategies, institutions, and trained personnel strengthens resilience and reduces global vulnerabilities.
- **Tailor support to real needs:** Demand-driven, transnational and public-private approaches ensure capacity building has lasting impact.
- **Workforce and civic engagement matter:** Defining cyber jobs, filling talent gaps, and mobilizing civic initiatives are essential to meet rising threats.



We look forward to welcoming you to the upcoming

MCSC MUNICH CYBER SECURITY CONFERENCE 2026