

CONFERENCE REPORT

 **MCSC** MUNICH CYBER SECURITY
CONFERENCE **2026**

MUNICH CYBER
SECURITY CONFERENCE

MCSC WAS ORGANIZED BY SECURITY NETWORK MUNICH AND ITS PARTNERS.

MEET THE MCSC CORE TEAM 2026:



Peter Moehring
Managing Director
Security Network Munich



Antje Hickethier
PR and Event Management
Security Network Munich



Roberta Walser
Partnerships & Development
Security Network Munich



Kai Hermesen
DECAID Secure



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



Marc Raimondi
Chief of Staff, Silverado
Policy Accelerator



John Mengersl
Founder and Executive
Director of C-Suite Advisor



Nicole Tisdale
Interim Senior Director
to the Cybersecurity
Programs, Aspen Digital

AUTHORS:



Niklas Zimmer
Junior Program Officer in the Digital Program of the
Aspen Institute Germany

Niklas Zimmer is a Junior Program Officer in the Digital Program of the Aspen Institute Germany. In this role he manages projects focused on cybersecurity and strengthening democratic resilience online through combating the spread of disinformation and foreign information manipulation and interference (FIMI). Prior to joining the Digital Program, Niklas worked for various NGOs, international organizations, and served as a research assistant in the Department of Communication at the University of Vienna. His research interests include hybrid warfare, digital governance, and democratic cohesion. Niklas holds a B.A. in Political Science and a B.A. in Mass Media and Communication Science from the University of Vienna. Currently, he is completing his Master's in International Affairs with a focus on International Security at the Hertie School of Governance, supported through a scholarship from the Heinrich Böll Foundation.



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.

This report was also developed with the support of Molly Hall.



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 produced by Security Network Munich in cooperation with Aspen Institute Germany. All rights reserved by Security Network Munich.



MUNICH CYBER SECURITY CONFERENCE 2026

Command Control, Really?

Confronting The Illusion Of Deterrence
In The Age Of Relentless Cyber Threats.

Patronage:

Bavarian Ministry of Economic Affairs,
Regional Development and Energy



Supported by:



Institutional Partners:



EXECUTIVE SUMMARY

The digital domain has evolved beyond being a central pillar for security and economic growth to an arena for geopolitical competition. Cybercrime, hybrid threats, and the accelerating employment of AI are reshaping the global cybersecurity environment. As digital infrastructures become increasingly critical to economies, governments, and democratic processes, strengthening resilience, safeguarding digital sovereignty, and rethinking cybersecurity approaches are emerging as fundamentally important questions and policy challenges.

In 2025, the economic damage inflicted by cybercrime reached an estimated \$10.5 trillion, according to Cybersecurity Ventures. Equivalent to roughly twice the GDP of Germany, these costs highlight the staggering scale of cyber-enabled crime, making it the most lucrative criminal enterprise globally. With the capacity to disrupt economies, damage critical infrastructure, and steal sensitive data, cyber operations have become a major security concern for governments and businesses alike. Concurrently, hostile states are launching their own cyber attacks while serving as sanctuary states for cybercriminal groups, enabling them to target foreign governments, companies, and institutions with limited risk of punishment.

In response, affected businesses and governments have sought deeper integration and cooperation. As part of this shift, cyber deterrence, defined as deterring potential adversaries through the threat or use of cyber capabilities, is increasingly moving beyond purely defensive measures toward more active and cost-imposing strategies. Alongside, actors in the cybersecurity sphere are grappling with the rapidly evolving nature of the threat landscape, particularly the transformative impact of artificial intelligence. According to the Global Cybersecurity Outlook 2026, 87 percent of respondents identified AI-driven threats as the most pertinent threat facing cybersecurity today.

These developments raise important questions about control, sovereignty, and agency in cyberspace that underpinned the discussions at the Munich Cyber Security Conference 2026, held under the title “Command Control, Really? Confronting the Illusion of Deterrence in the Age of Relentless Cyber Threats”. Over the course of two days, leading representatives from government, industry, academia, and civil society convened to discuss how best to respond to the evolving cyber threat landscape. This report summarizes the key discussions of the conference, providing analytical context through thematic deep dives and synthesizing the main takeaways of the event.

Across the discussions, several overarching insights emerged. Participants stressed that the cyber domain has entered a phase where defensive postures alone are no longer sufficient to manage systemic risks. Effective deterrence increasingly requires forward-defending strategies that raise the costs for malicious actors, while deeper integration between governments and the private sector has become essential for maintaining strategic advantage. At the same time, debates around digital sovereignty highlighted that control in cyberspace cannot be achieved through isolation, but through resilient infrastructures, trusted partnerships, and the ability to shape technological ecosystems. The rapid advancement of artificial intelligence (AI) further complicates this landscape, transforming both offensive capabilities and defensive strategies.

What emerged from the 2026 Munich Cyber Security Conference is a growing recognition that control in cyberspace is becoming harder to sustain. Rather than seeking absolute control, policy makers and practitioners must learn to operate in a domain defined by constant adaptation. In this environment, resilience will depend less on static defenses and more on the capacity to anticipate disruption, adapt quickly, and cooperate across sectors and borders.



KEY TAKEAWAYS

1. Cyber Deterrence Must Be Forward-Defending, Active, and Cost-Imposing

Unlike conventional military confrontation, cyber operations are often elusive, making attribution difficult and retaliation uncertain. This allows malicious actors to launch attacks with relatively low expected costs while potentially inflicting significant economic and societal damage on their targets. As a result, a structural asymmetry emerges that historically favors attackers and undermines the credibility of purely defensive deterrence strategies.

To address these asymmetries, several countries have updated their national cybersecurity strategies and adopted more active and forward-defending approaches. A prominent example is the United States, where U.S. Cyber Command has embraced a doctrine of “persistent engagement.” Under this approach, cyber operators seek to continuously contest adversaries in cyberspace by identifying threats early, disrupting malicious infrastructure, and degrading the capabilities of hostile networks before attacks reach critical systems. Countries heavily affected by cyberattacks such as South Korea and Japan followed suit adopting a similar active cyber strategy.

In Europe, the shift toward more active cyber deterrence has been more cautious. Governments have traditionally emphasized that cyber operations must remain firmly within existing legal frameworks and comply with international law. However, recent developments suggest a gradual move toward a more proactive stance. In early 2026, for example, the German government announced plans to propose legal changes that would expand the authorities of security agencies to conduct so-called “hack-back” operations, enabling them to disrupt malicious cyber infrastructure beyond their own networks.

Beyond actively disrupting the infrastructure of cybercriminals, cyber deterrence can alter the risk calculus for adversaries in multiple ways. The European Union’s Cyber Diplomacy Toolbox, for instance, enables member states to impose sanctions on individuals and entities responsible for malicious cyber activity, including travel bans to the EU and the freezing of financial assets. Such measures aim to increase the political and economic costs of cyber operations and signal that malicious behavior in cyberspace will carry tangible consequences. Through these cost-imposing and forward-defending approaches, cyber deterrence seeks to make hostile cyber activity more difficult, more expensive, and ultimately less attractive for potential attackers.

Due to the decentralized structure of the world’s digital infrastructure, private companies play a crucial role in enabling forward-defending deterrence. As they own and operate telecommunication networks, cloud services, and often entire software ecosystems, they possess unique visibility into cyber activities and are often the first to detect emerging threats. Recently, major technology companies have started to increasingly collaborate with government agencies, sharing threat intelligence, technical expertise, and operational capabilities to disrupt malicious cyber infrastructure. Operation Winter SHIELD in the United States reflects this logic, by encouraging intelligence sharing between the private sector and the FBI.

Despite the growing push for more active and cost-imposing cyber deterrence, critics emphasize the delicate balance between effectively disrupting malicious activity and safeguarding legal and privacy protections. Questions about the appropriate legal mandate for forward-defending operations repeatedly arise, particularly given that cyber operations often occur across jurisdictions and may affect infrastructure located in other states. Moreover, as private companies increasingly collaborate with government agencies, concerns about data protection, oversight, and the handling of sensitive information have become more prominent. How states navigate these legal and societal concerns while expanding forward-defending cyber strategies will remain a key question for the future of cyber deterrence.

2. Public-Private Integration Determines Strategic Advantage

The digital infrastructure underpinning modern economies is largely owned and operated by private actors, from cloud service providers and telecommunications companies to software developers and platform operators. As a result, cybersecurity has evolved beyond a purely governmental responsibility and increasingly depends on cooperation between public authorities and industry. This structural interdependence renders effective cyber defense unachievable by governments acting alone, but requires integrated approaches that combine the regulatory authority of the state with the technical capabilities and operational expertise of the private sector. Countries that succeed in aligning these complementary strengths are thus better positioned to anticipate threats, protect critical systems, and respond effectively to cyber incidents.

Public-private partnerships span a broad operational field and offer multiple pathways for cooperation. A report by the United Nations Office on Drugs and Crime (UNODC) highlights that such partnerships can support efforts across the entire cybercrime lifecycle, including detection, disruption, prosecution, and victim assistance. In practice, this cooperation often takes the form of threat intelligence sharing, joint disruptive operations against cybercriminals, capacity-building, and technical assistance for law enforcement.

Done right, public-private integration therefore constitutes an essential strategic asset and can tilt the power balance toward the defending side. Several countries have adopted strategies that reflect this logic by embedding

KEY TAKEAWAYS

public-private cooperation at the core of their cybersecurity policies. The United States, for instance, launched the Joint Cyber Defense Collaborative (JCDC) in 2021, establishing a framework for operational collaboration through intelligence sharing and coordinated responses to cyber threats. Demonstrating the effectiveness of this approach, the JCDC contributed greatly to securing the Paris Olympic Games, with U.S. companies monitoring emerging cyber threats and sharing relevant intelligence with France's Agence nationale de la sécurité des systèmes d'information (ANSSI) to support the protection of critical digital infrastructure. This example showcases that public-private partnerships do not have to be limited to the national context, but can also operate at an international level, where the interests of governments and companies align.

In Germany, public private partnerships have a long and successful tradition through the Allianz für Cyber-Sicherheit. As one of Europe's largest cybersecurity networks, the initiative enables threat intelligence sharing, and best practice exchange between Germany's largest private companies and the Federal Office for Information Security (BSI). Crucially, its effectiveness rests not only on technical cooperation but also on the trust built between participating actors. In a domain where timely information sharing and coordinated responses are essential, such trust-based relationships form a critical foundation for effective cybersecurity governance.

3. Sovereignty Means Strategic Control, Not Autarky

As digital technologies become increasingly essential to economic competitiveness, democratic governance and security, concerns over digital sovereignty have moved to the forefront of cybersecurity debates. Particularly in Europe, policy makers are reassessing their dependency on foreign technology, platforms, and supply chains by seeking to ensure that data flows, critical digital infrastructure, and technological capabilities remain in the hands of European companies.

This political push, emphasized by the recent Declaration for European Digital Sovereignty adopted in November 2025, comes at a time of increasing "weaponization of interdependence," as states leverage their market power to pressure adversaries and allies alike. In response, policy makers and businesses across Europe have begun exploring alternatives in key areas such as cloud services, software ecosystems, and digital infrastructure to ensure that future digital technologies align with European values. Denmark, for instance, has recently begun replacing Microsoft Office with LibreOffice, an open-source software solution developed in Europe, across several government ministries. Other actors, including parts of the Austrian armed forces, have pursued similar initiatives, reflecting a broader effort to reduce strategic dependencies in critical digital systems.

However, digital sovereignty does not equal digital autarky. In seeking to strengthen control over digital infrastructure and technology, policy makers and business executives must walk a tightrope between identifying areas where greater strategic control is needed and avoiding shutting oneself off completely. Modern digital supply chains are deeply interconnected, spanning multiple jurisdictions and involving a wide range of actors. Attempting to fully isolate national or regional digital systems would therefore risk undermining innovation, increasing costs, and fragmenting the global digital economy.

Ensuring a high level of cybersecurity requires both governments and businesses alike to carefully determine which tools and strategies are most effective in addressing specific risks. While open-source solutions and smaller technology providers can offer greater autonomy, transparency, and control over data, companies such as Amazon and Microsoft operate vast global infrastructures that benefit from significant economies of scale, allowing them to invest heavily in advanced threat detection, and large-scale incident response capabilities.

In this sense, digital sovereignty should not be understood as technological isolation, but as the ability to maintain strategic control over critical digital systems while still choosing the solutions that provide the most effective cybersecurity. For this reason, many organizations have adopted Zero Trust security architectures, which rely on continuous monitoring of their systems rather than assuming that they are inherently secure. At the same time, governments and businesses must carefully assess in which areas strategic sovereignty is necessary, and where cooperation with global technology providers can strengthen security.

4. AI Is Fundamentally Changing the Playing Field

Cybersecurity is undergoing several rapid transformations, few, however, are as impactful as the deployment of AI. For cyber criminals, AI enables the up-scaling of their criminal activity through automated campaigns, the identification of system vulnerabilities, and the employment of bots. These developments significantly increase the speed and sophistication of malicious cyber operations while lowering the entry barrier.

At the same time, AI also offers powerful tools for defenders. LLMs can analyze large volumes of data and detect anomalies, thus identifying potential threats far more quickly than the human eye. Private companies and government authorities have therefore begun integrating AI-based security applications into their cyber defense architectures, strengthening their response mechanisms to deal with the growing volume of attacks.

KEY TAKEAWAYS

Beyond the evolving balance between offensive and defensive applications, AI also raises fundamental questions for cybersecurity governance. Policy makers will have to grapple even more with questions of accountability, transparency, and the risks of automated decision-making. In order to address these questions, the European Union adopted the AI Act in 2024, establishing minimum requirements for companies to assess and manage risks arising from the use of AI in cybersecurity. Ensuring that governance keeps pace with the rapid evolution of AI will therefore remain a central challenge for legislators.

Taken together, these developments illustrate the profound transformation of the cybersecurity playing field driven by the advancement of AI. As both attackers and defenders increasingly integrate AI into their operations, the balance of power in cyberspace is likely to become even more dynamic and unpredictable. Maintaining an advantage in this environment will therefore depend not only on technological innovation, but also on the effective cooperation between governments and companies to adequately respond to the deployment of these new capabilities.

5. Cyber Security Is Economic Security

In today's digital economy, cybersecurity no longer constitutes a technical issue but is instead a fundamental pillar of ensuring economic growth and stability. Critical sectors such as energy and finance rely heavily on digital infrastructure to operate effectively. As a result, cyber attacks on these systems can significantly disrupt economic activity, not only leading to substantial financial losses but also causing broader ramifications for society as a whole.

Constituting one of the most lucrative criminal activities worldwide, cybercrime has grown exponentially in recent years. In Germany alone, cybercrime inflicted an estimated €267 billion in damages, with 81 percent of German companies reporting that they have been victims of cybercrime, according to a 2024 study published by Bitkom. Beyond imposing heavy costs on companies, cyber attacks can also result in reputational damage and the loss of consumer trust, thereby affecting firms far more broadly.

Cybersecurity challenges affect not only individual firms but extend across entire economic systems. Modern economic activity is deeply embedded in complex and highly interconnected digital supply chains, particularly in critical sectors such as transport, energy, and finance that form the backbone of economic activity. Disrupting these services thus constitutes a systemic risk that can have ripple effects extending beyond financial damage to the fundamental security of society as a whole.

In order to ensure long-term economic resilience, cybersecurity therefore represents a strategic priority for governments and businesses alike. Safeguarding critical digital supply chains and infrastructure will be essential for maintaining stable economic activity and public trust. Looking ahead, strong cybersecurity will increasingly form the foundation of sustainable economic growth and an important competitive advantage in the global digital economy.



CONFERENCE AT A GLANCE – THE MCSC IN NUMBERS

Participants: **1,000+**

Number of speakers: **100+**

Countries represented (incl. country of origin of speakers): **50+**

Continents represented: **5**

Number of sessions (panels, keynotes, special formats): **30+**



100+
Speakers

1000+
Participants

30+
Sessions

50+
Countries
represented

WELCOME:

Speaker: **Claudia Eckert**, Chairwoman Security Network Munich

In her capacity as the Chairwoman of the Security Network Munich, Claudia Eckert welcomed the participants to the 12th Munich Cyber Security Conference. She introduced this year's theme "Command Control, Really? Confronting The Illusion Of Deterrence In The Age Of Relentless Cyber Threats", explaining that the conference aimed to take a step back and provide a broader perspective on the current cybersecurity landscape. In this context, she suggested that the event should serve as a reality check, asking whether current approaches to cyber deterrence were sufficient or whether the belief in their effectiveness risked becoming an illusion amid an increasing number of cyber threats.

Eckert noted that these questions arose at a time of profound geopolitical transformation, with many countries reassessing their security architectures and redefining how security should be organized. She highlighted several key challenges shaping the cyber domain, including the economic impact of cyberattacks, the question of whether new law enforcement regulations were needed, and the rapidly changing risk landscape created by emerging technologies such as artificial intelligence. She emphasized that addressing these issues required open dialogue between stakeholders from different countries and sectors, which the Munich Cyber Security Conference seeks to foster by bringing together representatives from politics, academia, and the private sector.



Claudia Eckert:

"We have to ask ourselves is our deterrence just an illusion, as we have to cope with an increasing amount of cyber threats or do we have appropriate means to defend ourselves."



Europe's leading expert network for information security



The Security Network Munich (Sicherheitsnetzwerk München) is an association of leading players, organisations and research institutes in the field of information and cyber security in the greater Munich area. Our goal is to foster industry cooperation through joint research and innovation projects. Our members meet regularly to discuss pressing industry challenges with government and research institutions. We also convey the industry's insights and concerns to a political and broader societal audience, through education and communication, spreading awareness of the importance of information security.

Set up as a project funded by the Bavarian Ministry of Economic Affairs in 2012, the network founded the non-profit association "Sicherheitsnetzwerk München e.V." in January 2019. The association stands to promote cooperation and exchange among its members across different industries and academia, foster innovation projects and education initiatives directed especially to students and young adults. The Security Network Munich is committed to engage -together with its partners- in awareness and best practice campaigns with special emphasize on SMEs. Security Network Munich is a founding member of Ensure Collaborative, an international Network of Security Clusters.

For more information on the network and membership, please visit <https://security-network-munich.org>.

FIRESIDE WITH SEAN CAIRNCROSS:

Speaker: Sean Cairncross, National Cyber Director

Moderator: David Lashway, Sidley

The conversation between David Lashway and Sean Cairncross focused on the evolving cyber strategy of the United States and the role of partnerships in addressing the growing cyber threat landscape. Cairncross emphasized that the U.S. administration had adopted a more action-oriented approach to cybersecurity, reflecting a broader mandate to address national security challenges more directly. While the guiding principle of “America First” shaped this approach, he stressed that it did not mean the United States sought to act alone, noting that partnerships with allies remained essential.

Cairncross explained that the administration increasingly viewed cyberspace as a strategic domain requiring coordinated leadership across government. The U.S. cyber strategy, aligned with the National Security Strategy, aimed to shape adversary behavior while strengthening resilience and protecting critical systems. He highlighted the importance of cooperation with the private sector, noting that much of the world’s digital infrastructure was owned and operated by private companies. Effective cybersecurity therefore depended on close information sharing between government and industry as well as the ability of governments to use tools such as law enforcement and offensive capabilities to respond to malicious actors.

The discussion also addressed broader strategic questions, including the limits of purely defensive approaches to cyber threats. Cairncross noted that while resilience remained important, governments also had to consider how to impose costs on adversaries and respond more proactively to malicious activity. In closing, he emphasized that cyber threats affected all countries represented at the conference and that continued dialogue and cooperation among governments, industry, and international partners remained essential to strengthening collective resilience in the digital domain.

Sean Cairncross:

“Today, a lot of emphasis has been put on resilience but this means you are only observing shots; we need a mindset change, which means we work strategically not only in a reactive mode but collaboratively to make a dent in the space of the adversary and send a message that this behavior is unacceptable.”



PANEL 1: **Economies under Risk: What are we talking about?**

Speakers: Jürgen Reinhart, Chief Underwriter Cyber, Munich Re
 Jürgen Michels, Chief Economist, Bayerische Landesbank
 Livio Stracca, Deputy Director General, European Central Bank
 Molly Lesher, Head of Digital Connectivity, Economics & Society Division, OECD

Moderator: Barnabás Ferenczi, International Bankers Forum

The panel explored the growing economic dimensions of cyber risk, highlighting how cyber threats increasingly affect businesses, financial stability, and economic policy. Opening the discussion, Barnabás Ferenczi framed the debate by pointing to the rising financial scale of cybercrime, including estimates that global losses from cyber-enabled scams alone reached hundreds of billions of dollars annually. Several speakers reinforced this perspective with figures illustrating the magnitude of the challenge. Jürgen Michels noted that cyberattacks had caused an estimated €289 billion in damage to the German economy in the previous year, while also emphasizing that a large share of smaller firms had been targeted by cyber incidents. The discussion underscored that cybersecurity has become one of the most significant risks facing businesses worldwide.

A central theme of the discussion was the role of trust in the digital economy. Livio Stracca emphasized that sectors such as banking depended fundamentally on confidence in digital infrastructure and financial systems. As economic activity increasingly shifted online, cybersecurity had become a key condition for maintaining trust in digital transactions and financial stability, he argued. Similarly, Molly Lesher highlighted that cybersecurity should not be seen solely as a cost but as a foundation for productivity and economic growth. If users and companies lose trust in digital technologies, she argued, this could slow the broader benefits of digital transformation.

The panel also discussed structural challenges in understanding and managing cyber risks. Jürgen Reinhart pointed to the difficulty of measuring and pricing cyber risks, particularly given the complexity of digital supply chains and the many actors involved in operating digital infrastructure. Several speakers noted that cyber risks were often insufficiently reflected in corporate decision-making and market valuations unless a major incident had already occurred. Smaller firms in particular often underestimated the scale of the threat, even though they were frequently among the most vulnerable targets, according to the speakers.

Another theme of the discussion was the economic logic driving cybercrime. Panelists noted that many cybercriminal networks operated with business-like structures, seeking to maximize profits while minimizing the risk of detection. These actors responded to incentives much like legitimate firms, scaling operations, and recruiting talent to expand their activities. At the same time, some cyber operations were linked to geopolitical tensions and state-supported activities, complicating efforts to counter them through purely economic or law enforcement measures.

The panel concluded by reflecting on the broader systemic implications of cyber risk. As digital interdependencies deepened across sectors and borders, cyber incidents could potentially have cascading effects on economies and financial systems, highlighting the need for stronger coordination between policy makers, regulators, and industry.

The main takeaways from this panel were:

1. **Recognize cyber risk as an economic challenge:** Cybersecurity has become central to economic stability, productivity, and trust in digital systems.
2. **Improve the measurement and pricing of cyber risk:** Companies and markets still often underestimate cyber risks, particularly in complex digital supply chains.
3. **Address the incentives behind cybercrime:** Reducing the profitability of cybercrime and strengthening regulatory coordination will be critical to limiting its economic impact.



STRATEGY UPDATE FROM JAPAN:

Speaker: Yoichi Iida, National Cyber Director, Japan

Yoichi Iida outlined Japan's updated cybersecurity strategy, emphasizing the growing convergence of security challenges between Europe and the Indo-Pacific. He noted that both regions face similar threats to the rules-based international order, particularly from actors such as Russia, China, and North Korea. These challenges extend across digital security, cybersecurity, and economic security creating shared vulnerabilities for both Japan and Europe.

In response, Japan had shifted toward a more integrated and proactive approach to cyber resilience, Yoichi Iida highlighted. This included strengthening public-private partnerships and expanding international cooperation with like-minded partners. A key development was the government's enhanced ability to collect and analyze data from critical infrastructure operators and other sources, allowing for earlier identification of threats and more effective protective and mitigation measures. He emphasized that ensuring cybersecurity across entire processes and strengthening mission assurance was central to this approach.

Yoichi Iida also underlined Japan's commitment to deepening international collaboration, particularly in the Indo-Pacific. Through cooperation with ASEAN countries, Japan aimed to promote greater cyber resilience, improve threat awareness, and support responsible state behavior in cyberspace. He concluded by underlining that cybersecurity would play a central role in Japan's evolving national security strategy and expressing Japan's readiness to work closely with international partners to address shared challenges.



Yoichi Iida:

"We are determined to play a central role to build mutual trust, where we will also provide the private sectors with data collected by the government."



INTELLIGENCE VIEW: Cyber Space, the Future Arena Of Political Conflicts?

Speakers: Dag Baehr, Vice President, Federal Intelligence Service (BND), Germany
Paul M. Nakasone, Former NSA Director

Moderator: Paddy McGuinness, Brunswick Group

Governments face an increasingly contested cyber domain in which resilience alone is no longer sufficient and more active forms of deterrence are required. Both speakers stressed that while resilience remained an essential foundation for cybersecurity it had to be complemented by more proactive approaches to defense. At the same time, Dag Baehr warned that openly communicating capabilities or red lines could undermine deterrence by reducing uncertainty for adversaries.

A central theme of the exchange was the importance of cooperation across sectors. Paul Nakasone emphasized that governments could not secure cyberspace alone. Rather, effective responses depended on closer collaboration not only between states but also with the private sector, academia, and other actors operating in the digital domain. Information sharing was described as the starting point for such cooperation. Baehr similarly noted that many of the technologies and capabilities needed to address emerging cyber threats were concentrated in private companies, making strong public-private partnerships essential for scaling responses.

The conversation also highlighted the tension between technological interdependence and sovereignty. Baehr pointed out that much of the relevant technology remained concentrated in the United States, requiring European

Dag Baehr:

"We are at a structural inflection point because most of the technologies that are required to address the threats are not owned by government agencies."



actors to find ways to work effectively within this reality. Nakasone cautioned against digital decoupling, arguing that attempts to separate technological ecosystems could introduce new vulnerabilities. In a rapidly evolving threat landscape, both speakers stressed that faster information sharing and trusted partnerships were critical for managing future cyber conflicts.



TRANSATLANTIC VIEW: **Overcoming Borders–Disrupting Cyber Crime.**

Speakers: Catherine De Boller, Executive Director, Europol

Andrew Bailey, Deputy Director, FBI

Moderator: Carsten Meywirth, Director Cybercrime, German Federal Police Office

Cybercrime has evolved into a sophisticated global ecosystem in which criminal networks provide services such as botnets, bulletproof hosting, and money laundering infrastructure, creating a “crime-as-a-service” model that increasingly resembles legitimate digital business models. Both speakers emphasized that effectively disrupting these networks required shifting the focus from individual offenders to the infrastructure that enables large-scale criminal activity.

A central theme of the exchange was the importance of international cooperation. Andrew Bailey stressed that cybercrime was a borderless threat requiring close collaboration between governments, law enforcement agencies, and the private sector. Information sharing and coordinated operations were described as essential for responding quickly to evolving threats. De Boller highlighted the role of Europol as the EU’s criminal intelligence hub and pointed to operational task forces that bring together specialists from multiple countries to investigate complex cybercrime cases.

The conversation also highlighted how the cybercrime landscape has evolved in recent years. De Boller explained that the rise of cybercrime-as-a-service has lowered the barriers to entry for malicious actors who no longer need advanced technical expertise to conduct attacks. Both speakers also pointed to the geopolitical dimension of cybercrime, noting that some states tolerated or enabled criminal infrastructure. In response, governments had to increasingly target the broader ecosystem supporting cybercrime through coordinated law enforcement action, sanctions, and stronger international partnerships, Bailey argued.

Andrew Bailey:

“Cybersecurity is national security, it is public safety and economic security. Nation states that provide sanctuary for cyber criminals are putting themselves against the civilised world. This is why those partnerships are so important to attack those ecosystems.”



PANEL 2: **Offensive Defense: Legal Conundrum.**

Speakers: Florian Schütz, Director, NCSC, Switzerland
 Thomas Goger, Chief Public Prosecutor, Bavarian Cybercrime Prosecution Office
 Brett Leathermann, Director, FBI Cyber Group
 Sandra Joyce, VP Threat Intelligence Group, Google

Moderator: Marc Raimondi, Silverado

The panel examined whether more proactive cyber defense measures are necessary and how such approaches can operate within existing legal frameworks. Speakers emphasized that cyber threats increasingly blurred traditional distinctions between offense and defense. Brett Leathermann noted that “active defense,” a term often used in the private sector, typically referred to taking actions within an organization’s infrastructure, such as creating traps for malicious actors or gathering intelligence.

A central theme of the discussion was the need to move from intelligence sharing to operational disruption. Sandra Joyce highlighted recent operations in which intelligence gathered on malicious infrastructure was used to coordinate takedowns of cybercriminal networks in cooperation with partners. Thomas Goger added that law enforcement agencies increasingly attempted to infiltrate criminal command-and-control structures in order to identify and prosecute the individuals behind cyber operations.

The panel also discussed the legal and political constraints shaping cyber responses. Florian Schütz emphasized that governments had to operate within clear legal frameworks, including intelligence, military, and law enforcement authorities, while maintaining checks and balances that distinguish democratic responses from the behavior of cybercriminals. Concurrently, the discussion highlighted the structural challenges posed by cyberspace being largely privately owned infrastructure, which required close cooperation between governments and companies.

The conversation concluded by emphasizing that more proactive approaches were necessary to counter increasingly sophisticated cyber threats. While attribution, sanctions, and law enforcement actions remained important tools, several speakers argued that deterrence ultimately required raising the costs for attackers by disrupting their infrastructure, financial flows, and operational capabilities.

The main takeaways from this panel were:

1. **Recognize cyber risk as an economic challenge:** Cybersecurity has become central to economic stability, productivity, and trust in digital systems.
2. **Improve the measurement and pricing of cyber risk:** Companies and markets still often underestimate cyber risks, particularly in complex digital supply chains.
3. **Address the incentives behind cybercrime:** Reducing the profitability of cybercrime and strengthening regulatory coordination will be critical to limiting its economic impact.



EXECUTIVE VIEW: **Offensive Defense: Legal Conundrum?**

Speakers: Tom Leighton, Co-Founder and CEO of Akamai
Tomer Weingarten, Co-Founder and CEO of SentinelOne

Moderator: Alexander Schellong, Executive Management Board, Schwarz Digits

The Executive View explored the lessons from building cybersecurity companies and the challenges of innovating in a highly competitive and adversarial environment. Tom Leighton emphasized that persistence was essential for entrepreneurs tackling difficult problems. Founders had to be prepared to face skepticism and criticism, but should listen carefully without simply following the advice of others. He also encouraged entrepreneurs to think creatively and remain open to unconventional ideas when addressing complex security challenges.

Tomer Weingarten reflected on the importance of purpose and conviction when founding companies in the cybersecurity sector. In cybersecurity, defenders were constantly competing with adversaries who quickly copied and adapted new developments. Therefore, establishing long-term commitment and a strong sense of mission was essential.

The conversation also highlighted the transformative role of new technologies in software development. Both speakers noted that advances in generative AI tools were lowering the barriers to coding, allowing more people to build complex digital systems even without traditional programming backgrounds. While this democratization of coding created new opportunities for innovation, it also reinforced the need to design digital infrastructure with security in mind from the outset.

Tom Leighton:

“If you want to do something important, there will always be a lot of naysayers. Listen to them, but do not just blindly execute what they say. Do not be afraid of thinking out of the box. Keep your eyes and ears open, and keep your brain turned on.”



SPOT-ON: (Re)Interpreting (Cyber)Risk.

Speakers: Christopher Ahlberg, Co-Founder of Recorded Future
 Miguel de Bruycker, Director-General, CCB, Belgium
 Louise Marie Hurel, Senior Researcher, RUSI
 Alex Fitzsimmons, Acting Under Secretary of Energy, U.S. Department of Energy

Moderator: Geoff Brown, CEO Silobreaker

The conversation examined how the cyber threat landscape is evolving and how governments and companies should interpret emerging risks. Christopher Ahlberg noted that cyber threats were constantly shifting, pointing to changes in tactics of threat actors. For example, North Korea had increasingly moved from directly financing cybercrime to embedding thousands of operatives in companies. Meanwhile, ransomware groups operating as spider-like organizations outside Russia were becoming a more prominent threat. Louise Marie Hurel highlighted that debates on cyber attribution were also evolving, with non-Western governments such as China and Singapore becoming more vocal in attributing cyber activity. Understanding how different countries approached attribution and deterrence, she argued, was essential for navigating an increasingly complex geopolitical landscape.

Several of the speakers emphasized the importance of proactive defense and operational responses to cyber threats. Miguel de Bruycker, for example, described how Belgian authorities issued tens of thousands of warnings to organizations informing them that their vulnerabilities were actively being exploited, thus helping contain ransomware incidents by encouraging early action.

The exchange also highlighted the growing importance of international and multi-stakeholder cooperation and information sharing. Ahlberg emphasized that cyber threats did not stop at national borders and that the most valuable intelligence might come from partners far beyond a country's immediate neighborhood. At the same time, several speakers noted the importance of trusted partnerships between governments and companies, as critical infrastructure was largely in private ownership. Alex Fitzsimmons, for example, stressed that the energy sector required greater attention from policy makers. According to him, energy systems formed the backbone of modern economies, where large portions of the infrastructure are privately owned.

Finally, the speakers discussed the future of cooperation in an increasingly fragmented geopolitical environment. While some participants expressed optimism that technological tools and alliances would make information sharing easier, Hurel took a more cautious view, warning that rising geopolitical tensions and competing notions of digital sovereignty could complicate collaboration. Despite these challenges, the discussion underscored that trust, shared platforms for cooperation, and stronger partnerships across governments and industry remained central to managing cyber risks in the years ahead.



KEYNOTE: Responding to the Current Threat Landscape.

Speaker: Lisa Gustafsson, Director of Foreign Intelligence and Cyber at the Swedish Ministry of Defence



Speaking from a Swedish perspective, Lisa Gustafsson outlined how the cyber threat landscape is rapidly evolving, emphasizing that cyber operations were increasingly intertwined with geopolitical conflict. She noted that Russia's invasion of Ukraine had fundamentally altered Europe's security environment, with cyberattacks becoming a central tool of modern warfare. In response, she stressed that Sweden was strengthening its defense posture and cybersecurity strategy to ensure credible deterrence.

Gustafsson highlighted that the focus of defense had shifted from physical infrastructure to digital systems, with cybersecurity now

Lisa Gustafsson:

"The threat landscape is changing fast. This is the reality we must respond to."



playing a dual role: Protecting critical infrastructure in everyday operations while ensuring functionality in times of crisis and conflict. She explained that Sweden's model was based on shared

responsibility across government, private sector, academia, and public authorities, reflecting the reality that much of critical infrastructure was privately owned and increasingly digitalized.

Concluding, Gustafsson warned against assuming that cyber disruptions will remain isolated or limited. Instead, she emphasized the need to build resilience at scale, including managing both technical and non-technical risks and strengthening long-term capabilities through research and innovation.

PANEL 3: Risk Management Reset: Change of Mindset.

Speakers: Lars Koenig, Head of Detection and Response, Allianz
Jonathan Ellison, Director National Resilience, NCSC, UK
Richard J. Watson, Global Cybersecurity Leader, EY
Claudia Plattner, President, Federal Information Security Agency, Germany

Moderator: Kiersten Todt, SVP Cybersecurity, Mastercard

The panel examined how cyber risk management is evolving as threats become faster, more complex, and consequential for societies and economies. As low detection rates and high financial rewards favored attackers, a change of mindset was necessary on the defenders side, the panelists agreed.

Lars Koenig argued that traditional risk management approaches struggled to keep pace with the speed of the cyber threat landscape. Building on this, Claudia Plattner stressed that management boards had to recognize cybersecurity as a strategic risk, noting that the window between vulnerability disclosure and exploitation often shrunk to minutes. This was even more important as cyber attacks increasingly targeted critical infrastructure sectors, disrupting essential services and requiring complex recovery efforts, Jonathan Ellison added.

At the same time, several of the speakers highlighted the tension between regulatory compliance and effective security. Richard J. Watson warned that many companies treated compliance frameworks as an end in themselves, even though meeting regulatory standards did not necessarily ensure safety. Koenig similarly noted that compliance had to be understood as a baseline rather than proof of security. To improve regulatory approaches, Plattner suggested that governments had to work even more closely with industry, pointing to initiatives such as cooperation with major German companies through the "DAX 40 Cyber Nation" group.

The discussion also emphasized the growing importance of speed and technology in cyber defense. Watson noted that attackers could often move through systems within minutes, requiring organizations to shift from periodic risk assessments to continuous monitoring. Several of the speakers highlighted the potential of AI to analyze large volumes of data and accelerate threat detection, although Watson cautioned that companies often deployed AI

primarily to reduce costs rather than to expand defensive capabilities.

The main takeaways from this panel were:

1. **Cyber risk management must become faster and more strategic:** Organizations need continuous monitoring and stronger board-level engagement to respond to rapidly evolving threats.
2. **Compliance alone does not ensure security:** Regulatory frameworks provide a baseline, but resilience requires operational readiness and faster detection capabilities.
3. **Stronger cooperation and proper technology use are essential:** Effective cyber risk management depends on closer collaboration between governments and companies, supported by data sharing and technologies such as AI.



PANEL 4: **Standing on the Shoulders of (Tech) Giants: Truth or Dare?**

Speakers: **Martin Merz**, President Sovereign Cloud, SAP
Rolf Schumann, Co-CEO, Schwarz Digits
Andrea Campora, ECSO Chairperson, Managing Director Leonardo Cyber & Security Solutions Division
Amy Hogan-Burney, CVP Customer Security & Trust, Microsoft
Markéta Gregorová, Member of European Parliament

Moderator: **Gabriel von Mitschke-Collande**, Group CDO Giesecke+Devrient

The panel explored how digital sovereignty can be achieved in an environment dominated by large technology providers. Markéta Gregorová argued that sovereignty should not be understood as complete independence, but rather as diversification. Building resilience required layered approaches, including greater use of open-source solutions and alternative providers to reduce dependency on a small number of companies. Similarly, Martin Merz noted that digital sovereignty should be understood as maintaining freedom of choice and control rather than building entirely independent systems. This involved combining best-in-class global technologies with targeted investments in domestic capabilities.

Several speakers highlighted the tension between dependence on global technology firms and the need for control over critical systems and data. Andrea Campora emphasized that sovereignty without capability remained an empty concept, suggesting that Europe had to partner with major technology providers while developing its own capabilities in key areas. Rolf Schumann similarly stressed that certain areas – particularly data – should remain under European control, arguing that organizations should not rely entirely on external providers.

The discussion also addressed the role of regulation in shaping the digital ecosystem. Amy Hogan-Burney emphasized that regulators played a key role in structuring the technology landscape but warned that overly burdensome regulation could hinder innovation. Gregorová argued for a more differentiated approach, suggesting stricter rules where personal data was involved while allowing greater flexibility in other areas. At the same time, Amy Hogan-Burney noted that existing frameworks such as GDPR could create challenges for information sharing, particularly in the context of cybersecurity and threat intelligence.

Across the discussion, speakers agreed that achieving sovereignty required a balance between cooperation, regulation, and strategic investment.

The main takeaways from this panel were:

1. **Sovereignty requires diversification, not isolation:** Reducing dependency on single providers through layered and diversified approaches strengthens resilience
2. **Control and capability must go hand in hand:** Strategic autonomy depends on combining partnerships with investments in key domestic capabilities
3. **Trust and regulation must be balanced with innovation:** Effective governance requires transparent frameworks that protect data while enabling technological progress.



GREETING STATE SECRETARY:

Speaker: **Tobias Gotthardt**, Bavarian Ministry of Economic Affairs



To conclude the first day of the conference, Tobias Gotthardt expressed his appreciation to the Munich Security Network for organizing the event and bringing together a diverse international group of participants. He emphasized that cybersecurity had become a central societal and economic challenge, with cyberattacks no longer being marginal phenomena but causing significant damage across both industry and critical infrastructure. In Germany alone, he noted, cyber incidents had resulted in economic losses amounting to hundreds of billions of euros.

Tobias Gotthardt:

“This year again, the MCSC is playing an important role in ensuring a secure digital future. One of this conferences greatest strengths is its international perspective.”



Tobias Gotthardt highlighted that cyber threats were becoming more frequent, faster, and increasingly sophisticated, with AI lowering barriers for cybercrime and fundamentally reshaping the threat landscape. At the same time, cyber operations were no longer driven solely by financial motives but were increasingly linked to political objectives. In response, closer cooperation between governments, industry, and civil society was needed. He concluded by underlining the importance of international exchange and dialogue, noting that formats such as the Munich Cyber Security Conference played a crucial role in strengthening collective efforts to secure the digital future.

BREAKOUT 1: **Tech Sovereignty and Trusted Technology: Two Sides of the Same Coin?**

Speakers: **John Miller**, General Counsel and Senior Vice President of Policy, ITI
Despina Spanou, Deputy Director-General, DG CNECT, European Commission

Moderator: **John Higgins**, Chair, International AI Governance Association

The discussion examined the evolving concept of digital sovereignty and its relationship to trust in technology. In this context, Despina Spanou emphasized that sovereignty in the digital domain could not be achieved by individual actors alone but required collective action, particularly given growing dependencies in global supply chains. She highlighted the EU's approach of "de-risking," which aimed to reduce vulnerabilities through risk-based assessments of suppliers while remaining open to those complying with EU standards.

John Miller provided a more critical view. Pointing to the challenges posed by the absence of a global definition of digital sovereignty, he argued that the subsequent ambiguity complicated implementation and risked fragmenting markets. He suggested reframing the debate around trust as a more practical concept. Responding to concerns about fragmentation, Despina Spanou argued that the EU had demonstrated its ability to act collectively in key areas, emphasizing that greater coordination strengthened unity.

Widening the lens, the speakers also addressed broader questions of trust, regulation, and market dynamics. John Miller noted that public trust in technology was often shaped by national regulatory frameworks, cautioning against reducing sovereignty debates to geography. Despina Spanou highlighted ongoing efforts to define high-risk suppliers and refine regulation, including initiatives on cloud and AI governance.

Overall, the exchange showed that achieving technological sovereignty depends on balancing openness with security while building trust across governments, industry, and international partners.



BREAKOUT 2: **A New Threat: Resisting Algorithmic Propaganda.**

Speakers: **Andrius Kubilius**, European Commissioner for Defence and Space
Mykolas Katkus, Founder, Repsense
Günther H. Oettinger, President, United Europe
Ghee Leng, Founder, Embedded LLM

Moderator: **Oliver Rolofs**, Co-Founder, MCSC, Managing Director, Commvisory

The panel explored how algorithm-driven information environments are reshaping the nature of propaganda and democratic resilience. Günther H. Oettinger emphasized that Europe had to strengthen its digital sovereignty, including through common standards, stronger regulation, and greater control over its own platforms and content ecosystems. He warned that without a more unified and strategic approach, Europe risked remaining dependent on external actors while facing growing pressure from geopolitical competitors.

Particular attention was given to the scale and mechanics of algorithmic propaganda. Drawing on empirical data, Mykolas Katkus highlighted how social media platforms such as TikTok and Telegram had become key channels for the dissemination of coordinated narratives, often originating from state-linked actors. He explained how content could move from niche platforms into mainstream channels, where algorithms rapidly amplified it beyond control.

This created “blind spots” in the information environment, where users struggled to distinguish between authentic and manipulated content. Andrius Kubilius reinforced this point by arguing that algorithmic manipulation had to be understood as a core security challenge, requiring not only regulation but also operational capabilities to detect, track, and respond to coordinated influence campaigns in real time.

The discussion also addressed the role of AI in both enabling and countering these dynamics. Ghee Leng warned that AI systems themselves could be manipulated through techniques such as “context poisoning,” undermining trust in digital information ecosystems. As AI-generated content became more pervasive, distinguishing between authentic and synthetic information would become increasingly difficult. The speakers therefore stressed that defense against algorithmic propaganda also needed to be AI-driven, combining technological tools with policy responses. Kubilius concluded that speed, coordination, and the ability to act decisively were critical, as democratic systems had to adapt to a reality in which information manipulation is continuous, scalable, and strategically deployed.



BREAKOUT 3: Asian Perspectives in a Fragmenting Digital World: Tech Sovereignty and Data Security.

Speakers: Yuh-Jye Lee, Senior Advisor, National Security Council, Taiwan
 Jeff Greene, Distinguished Fellow, Aspen Digital – Aspen Institute
Lead Commentator: Noboru Nakatani, Corporate EVP & CSO, NEC

Managing data across borders has become a central strategic challenge in today’s digital environment. Yuh-Jye Lee highlighted that for Taiwan, complete control over data was neither feasible nor aligned with economic realities, as both the public and private sector relied heavily on global platforms and infrastructures. Instead, the focus was on ensuring continuity and security, for instance through external data backups and trusted cooperation with international providers. This reflected a broader shift in thinking, where resilience and preparedness were prioritized over strict territorial control, Yuh-Jye Lee argued.

Furthermore, the conversation questioned whether technological sovereignty can meaningfully be defined in a globalized system. Jeff Greene argued that modern technologies were inherently transnational, with development, storage, and operations distributed across multiple jurisdictions. Efforts to localize systems too rigidly could therefore create new vulnerabilities rather than reduce them. In this context, sovereignty was framed less as ownership and more as the ability to make informed decisions about data, infrastructure, and risk exposure within complex global networks.

The increasing integration of AI added another layer of complexity. Lee pointed to the growing gap between rapid adoption of AI tools and limited awareness of their implications, particularly regarding privacy and data use. At the same time, Greene noted that neither governments nor companies were fully able to control how users engage with these technologies, as switching between platforms remained easy and largely unregulated. As a result, the panel suggested that future approaches to data security needed to combine technical safeguards with greater user awareness and more flexible, internationally coordinated governance.



BREAKOUT 4: MSC Startup Hub “A New Hope for Cyber Sovereignty?”

Speaker: Philipp Gerbert CEO, TUM Venture Labs



Philipp Gerbert highlighted a convergence of three key dynamics in cybersecurity: the growing relevance of security and defense, the rise of agentic AI as a “survival technology,” and the need to build startups that address challenges related to knowledge security.

Against this backdrop, Philipp Gerbert presented the MSC Startup Hub as a joint initiative between the Munich Security Conference, the Munich Cyber Security Conference, and TUM Venture Labs, positioning it as a new actor in the deep tech ecosystem.

He highlighted TUM’s strength as a leading university in computer science and emphasized that advancing deep tech innovation required close collaboration with the private sector: Based in Munich, the hub benefited from a uniquely integrated ecosystem in which universities, corporates, startups, and government actors are closely connected, enabling the creation of approximately 2–2.5 startups per week and contributing €2–2.5 billion in venture capital annually. Established six years ago, TUM Venture Labs focused on building domain-specific labs in twelve strategic fields, each led by managing directors with both technical and entrepreneurial expertise, with the aim of strengthening Europe’s deep tech capabilities. Gerbert stressed the importance of a flat, interdisciplinary structure and close collaboration across teams.

NEW THREATS: (One) Technology to Solve Them All?

Speakers: Pawel Rybczyk, CEO, Labyrinth
Ben Kliger, CEO, Zenity.AI
Torben Leowald, Clandestine Technologies
Kseniia Semenova, President, NAU

Moderator: Sarah Theinert, TUM Venture Labs

Emerging technologies, particularly AI, are fundamentally reshaping both cyber threats and defense strategies. Drawing on Ukraine's frontline experience, Kseniia Semenova highlighted that modern attacks combined cyber, physical and psychological elements, targeting not only infrastructure but also public perception. She described how coordinated campaigns linked missile strikes, disruptions of communication systems, and information operations to influence civilian behavior and decision-making. This evolution, she argued, required a broader approach to cybersecurity, including education in psychology, information security, and cyber diplomacy.

A key focus was how organizations can respond to increasingly complex and scalable threats. Pawel Rybczyk argued that traditional defensive approaches were becoming obsolete, as AI enabled attacks at scale and rendered static deception techniques ineffective. He instead advocated for a proactive, "preemptive" model of cybersecurity that anticipates and disrupts adversaries before attacks unfold. Ben Kliger pointed to the rapid rise of AI agents across corporate environments, noting that these systems already operated autonomously across business functions, access sensitive data, and interact with multiple services. This development challenged existing security architectures, which were originally designed around human users.

Broader structural and geopolitical implications also shaped the discussion. Torben Leowald highlighted the growing gap between technological innovation and regulatory frameworks, warning that overly restrictive regulation could limit Europe's ability to compete globally. Kseniia Semenova, in turn, underscored the practical limits of technological sovereignty, noting that even in conflict situations, countries remained dependent on external providers and had to balance security with cost and availability.

Finally, the speakers emphasized that adapting to this evolving threat landscape required not only new technologies, but also greater flexibility, stronger partnerships, and a shift toward more anticipatory security strategies.



BREAKOUT 5: MSC Startup Hub. The Scale Awakens. From Breakthrough to Deployment: Why Europe Lacks Cyber Champions.

Speakers: Tobias Lieberum, CEO, CyberDesk
Fabian Veit, CEO make.com
Joanna Swiatkowska, Secretary General, ECSO
Lennart Bock, COO, Proxima Fusion
Igor Andriushchenko, Head of Security, Lovable

Moderator: Sarah Theinert, TUM Venture Labs

Europe's difficulty in producing globally leading cybersecurity companies stood at the center of this breakout discussion. Tobias Lieberum pointed out that the challenge was less about technological capability and more about structural conditions, including limited investment and a lack of experience in working with startups. While innovative solutions were being developed, both Tobias Lieberum and Joanna Świątkowska emphasized that a persistent investment gap and the fragmentation of the European market were severe hurdles for startups to grow into scale-ups.

Bridging the gap between innovation and market success emerged as another key issue. According to Fabian Veit, companies succeeded when they deeply understand customer needs and offered transparent, reliable solutions, rather than overpromising. Yet, European firms often struggled to gain traction, as buyers frequently turned to established providers from the United States or Israel.

Beyond funding and market structures, the conversation pointed to deeper cultural and strategic factors. Lennart Bock emphasized that building deep tech companies required both significant capital and the ability to operate quickly while remaining secure, particularly in highly interconnected environments. More broadly, the speakers called for a shift in mindset: greater risk tolerance, stronger collaboration across the ecosystem, and a more deliberate effort to support European solutions. Without these changes, Europe risked continuing to generate innovation without successfully translating it into global leadership.



SPOTLIGHT: Cybersecurity in Kenya.

In recent years, Africa has undergone a rapid technological and digital transformation, contributing to the emergence of an increasingly dynamic digital ecosystem. Often referred to as the “Silicon Savannah,” Kenya has been at the forefront of this shift, establishing itself as a regional hub for technology and innovation. Major global technology companies such as Microsoft, Amazon, and Meta, alongside a growing start-up ecosystem, have made significant investments in the country, with the mobile money sector emerging as a key driver of economic activity and digital inclusion.

As Kenya’s digital sector has grown in importance, it has also become an increasingly frequent target of cyberattacks. Between April and June 2025 alone, a staggering 4.5 billion cyber threat events were recorded, resulting in estimated losses of roughly €200 million, according to different sources. Cybercrime has consequently risen to the top concern for businesses in East Africa, with a survey from PwC indicating that 74 percent of businesses view cyber risks as their primary concern, ahead of factors such as geopolitical risks.

In order to ensure economic and societal stability, cybersecurity has emerged as a top priority for Kenya. Thus, the government has strengthened both its domestic efforts and its engagement in international cyber diplomacy. Guided by its National Cybersecurity Strategy (2022-2027), Kenya has sought to enhance its capacity by announcing the establishment of a new National Cybersecurity Agency, while also strengthening and adapting existing institutions to support cybersecurity efforts, including the Kenya School of Government (KSG) and the Office of the Data Protection Commissioner (ODPC).

At the international level, Kenya has sought close cooperation with the EU, as reflected in the recent launch of the joint project Strengthening the Resilience of the Cybersecurity Ecosystem of Kenya (KCR), which has a budget of €3 million over three years. The project aims to enhance the security of Kenya’s digital sector by promoting cybersecurity capabilities and awareness. As an initial step, the Kenyan government has signed a Memorandum of Understanding (MoU) with Romania to deepen cooperation in cybersecurity, including partnerships with Romanian companies such as Safetech Innovations.

Overall, Kenya’s trajectory illustrates both the opportunities and challenges of rapid digital transformation. While the country has positioned itself as a regional leader in innovation and digital services, rising cyber threats underscore the need for sustained investment in resilience and governance. Continued efforts to strengthen domestic capabilities, combined with strategic international partnerships, will be essential to ensure that Kenya’s digital growth remains secure, inclusive, and sustainable in the years ahead.



THE MORNING BRIEF WITH KAUPU ROSIN:

Speaker: Kaupo Rosin, Head of Intelligence Service, Estonia

Moderator: Oliver Rolofs, Co-Founder, MCSC, Managing Partner, COMMVISORY

In conversation with Oliver Rolofs, Kaupo Rosin emphasized that cyber operations had become a core tool of intelligence and statecraft. From Estonia's perspective, Russia remained the primary threat actor, with no genuine indication of a shift toward peace. While Rosin stated that there was currently no active intent to launch a conventional attack on NATO, Russia continued to modernize its military and shape the threat environment along NATO's borders.

Rosin highlighted the growing importance of cyber capabilities for intelligence collection, noting that over half of Estonia's intelligence inputs now came from cyber sources. At the same time, he pointed to a gap between data collection and analysis, with much of the available data remaining unused without advanced tools such as AI. He also called on Europe to invest more in its own cyber capabilities, including offensive tools, and noted a shift toward smaller, more flexible cooperation formats between intelligence services.

Finally, Rosin described open-source intelligence as a useful but secondary tool that supports other intelligence disciplines. Reflecting on Estonia's experience, he noted that while the scale of cyberattacks had increased significantly, many successful intrusions still resulted from basic vulnerabilities. Strengthening cyber hygiene and access control therefore remained one of the most effective defenses against current threats.

Kaupo Rosin:

"We do not see active intent to launch a conventional attack on NATO but we have to work every day and invest in our external security and internal security in order to main this situation for the future."



VANTAGE POINT:

Speaker: Josephine Mwanzia, Senior Director Academic Affairs,

Kenya School of Government on Capacity Building in Public Administration

Josephine Mwanzia highlighted the importance of cybersecurity and digital transformation for public administration in Kenya, emphasizing that digitalization presented both opportunities and risks for social and economic development. She noted that strengthening cybersecurity was essential for protecting the digital economy and ensuring that public institutions are equipped to respond to cyber threats. In this context, the Kenya School of Government (KSG), which is celebrating its centenary, played a central role as a flagship institution for capacity building within the public sector in Kenya, she argued.

Josephine Mwanzia:

"In Kenya, we believe that the digital transformation presents challenges and opportunities which can be explored to enhance social and economic development."

Josephine Mwanzia outlined how KSG supports this effort through training, research, and innovation, including the establishment of specialized units such as a security management institute and an intelligence and research lab developed in cooperation with public and

private partners. These initiatives aimed to provide real-time data, enhance government responsiveness to cyber incidents, and strengthen digital literacy across public service. She emphasized that capacity building had to be continuous, equipping public officials with the skills, mindset, and tools needed to serve citizens effectively and ensure resilient governance in an increasingly digital environment.



The World's Largest Honeypot: Lessons Learnt from the Taiwan Cyber Battlefield.

Speaker: Yuh-Jye Lee, Senior Advisor, National Security Council, Taiwan

Yuh-Jye Lee emphasized that cybersecurity had evolved beyond a purely technical issue into a fundamental pillar of national and societal security, increasingly shaped by artificial intelligence and hybrid warfare. Drawing on Taiwan's experience as one of the most heavily targeted regions in cyberspace, he described the country as a "honeypot" for cyber operations, where threat actors continuously tested and refined their capabilities. He highlighted that cyberattacks were no longer limited to isolated incidents but increasingly targeted critical infrastructure, including energy and water systems, with examples of attacks linked to Chinese state-affiliated actors demonstrating the strategic intent behind these operations.

Lee stressed that the scale and sophistication of cyber threats were growing, with adversaries positioning themselves for potential future conflicts. In this context, cyberattacks on critical infrastructure had to be understood as a real and immediate risk rather than a hypothetical scenario. He argued that responding to these challenges required imposing tangible costs on malicious actors and strengthening deterrence. Referring to recent warnings issued by Taiwan's National Security Bureau regarding risks associated with certain digital platforms, he underscored the need for greater awareness and coordinated responses. As cyber warfare continued to evolve, Lee concluded that governments had to adapt to a landscape in which technological innovation and geopolitical competition are increasingly intertwined.

Yuh-Jye Lee:

"Defense alone is not enough. It does not suffice to build a wall if the adversary might already be in the building."



Across Borders: Cyber Diplomacy Needed More than Ever!

Speakers: Luca Tagliaretti, Director General ECCC
 Martin Koyabe, Senior Advisor, GFCE Africa
 Anny Vu, Senior Bureau Official, U.S. Department of State
 Felix Kroll, Cyber Coordinator, German Federal Foreign Office

Moderator: Katherine Getao, Cyber Ambassador and former Minister of Digital Affairs, Kenya

The panel highlighted how cyber diplomacy has become a central instrument for managing an increasingly contested digital domain. Anny Vu emphasized that cyberspace was a space of constant competition, with actors such as China, Russia, Iran, and North Korea seeking strategic advantage. She argued that reactive approaches were no longer sufficient and called for more active measures to impose costs on adversaries and reshape their behavior. At the same time, she stressed the importance of protecting critical infrastructure and strengthening cooperation with allies, as well as with industry and academia.

From a global perspective, Martin Koyabe noted that cyber diplomacy was becoming more inclusive, with more countries seeking to actively participate. He highlighted that issues of digital sovereignty – particularly control over data, cloud infrastructure, and AI – were increasingly shaping these international debates. Concurrently, regional actors such as the African Union were becoming more assertive in defining their role and interests in cyberspace.

Focusing on the European dimension, Luca Tagliaretti emphasized the importance of building trust across Member States and with industry. He pointed to ongoing efforts to support companies in adapting to regulatory requirements and to strengthen protection in critical sectors such as healthcare. Cross-border initiatives and cyber hubs were highlighted as key tools for enhancing coordination and improving situational awareness across the European Union.

Finally, Felix Kroll underlined the role of diplomacy in reinforcing international norms and ensuring accountability. While legal frameworks provided an important foundation, he argued that they had to be complemented by diplomatic tools such as sanctions and coordinated responses to influence adversary behavior. Across the discussion, speakers agreed that effective cyber diplomacy ultimately depended on strong partnerships, capacity building, and trust-based cooperation between governments, international organizations, and the private sector.



KEYNOTE:

Speaker: Radmila Shekerinska, Deputy Secretary General NATO



Radmila Shekerinska described a security environment defined by intensifying geopolitical competition, in which cyber operations have become a central instrument of state power. She pointed to Russia and China as key actors leveraging both traditional and emerging technologies to expand their influence, increasingly blurring the lines between civilian and military domains. Recent cyber incidents targeting critical infrastructure illustrated how digital attacks can translate into tangible societal and economic disruptions, underscoring the urgency of strengthening collective defenses, she argued.

In response, Radmila Shekerinska called for a more assertive and coordinated approach to cyber defense within NATO. This included significantly increasing investment in capabilities, integrating the cyber dimension into military planning, and ensuring that adversaries face meaningful consequences for malicious actions. At the same time, she stressed that effective cybersecurity could not be achieved by

Radmila Shekerinska:

“Both Russia and China are not only targeting us in the physical world but also in the digital world.”

governments or militaries alone, but depended on close cooperation with industry and other stakeholders. Strengthening resilience, accelerating response times, and acting collectively across the alliance were essential to maintaining security in an increasingly contested cyber domain.

KEYNOTE:

Speaker: Henna Virkkunen, Executive Vice-President, European Commission



Cybersecurity has become inseparable from overall security, as digital systems underpin economies, democracies, and critical infrastructure. Henna Virkkunen emphasized that in an era of heightened geopolitical tensions, cyberattacks, disinformation campaigns, and economic coercion were increasingly used to destabilize societies. Incidents targeting hospitals, supply chains, and essential services illustrated that cybersecurity was no longer a technical concern but a central pillar of Europe's security architecture. In response, she highlighted that the European Union had developed one of the most comprehensive cybersecurity frameworks globally and was strengthening institutions such as its cybersecurity agency to better support Member States and act internationally.

Strengthening Europe's resilience, she argued, required action across several areas, from mitigating supply chain vulnerabilities and securing 5G networks to improving cross-border coordination in response to threats such as drone incidents and infrastructure attacks. Virkkunen further stressed the importance of investing in European capabilities, including the development of a competitive cyber industry and stronger

Henna Virkkunen:

“We can no longer afford to be naïve about who can switch off our systems.”

defense capacities that integrate both civilian and military dimensions. Initiatives such as a cable security toolbox and expanded repair capacities were presented as concrete steps to protect critical infrastructure. Concluding, she underscored that Europe had to act collectively to remain secure, sovereign, and resilient in an increasingly contested digital environment.

Command Control, Really?

Speakers: General Michael Vetter, Director-General and CIO, German Armed Forces
General Rob Magowan, Commander Cyber Operations, UK Ministry of Defence
Katie Sutton, Assistant Secretary of War for Cyber Policy, U.S. Department of War

Moderator: Chris Painter, Former U.S. Diplomat

The panel emphasized that cyber operations had become an integral component of modern military strategy, particularly in the context of hybrid threats. Katie Sutton stressed that the complexity and speed of the cyber domain required militaries to move as fast as – or ideally faster than – their adversaries, making the integration of new technologies essential. She argued that cyber could no longer be treated as a siloed capability but had to be embedded across all levels of military operations, alongside closer cooperation with allies and the private sector. Michael Vetter reinforced this perspective, highlighting that hybrid attacks often targeted grey zones and critical interfaces, requiring a fully integrated security approach that included the military from the outset.

The discussion also addressed how cyber capabilities could be used to shape adversary behavior. Moving beyond a purely tactical mindset, Katie Sutton emphasized the need to integrate cyber into the broader instruments of national power. Credible deterrence, Michael Vetter argued, depended not only on capabilities but also on political will, including the readiness to escalate if necessary. In this context, hybrid operations, as highlighted by Rob Magowan, could be used strategically to distract, destabilize, or impose economic costs on adversaries, underlining their growing importance in contemporary conflict.

AI was identified as a decisive factor shaping future operations. Vetter described AI as essential for achieving information and decision dominance, warning that failing to adopt it would create a critical disadvantage. In a similar vein, Sutton emphasized the need to operationalize AI through close cooperation with industry, while ensuring its responsible use. However, Magowan cautioned that technology had to remain subordinate to operational objectives, stressing that human decision-making remained central despite increasing automation. Across the discussion, speakers agreed that future military effectiveness depended on the full integration of cyber capabilities with allied cooperation, technological innovation, and strategic coordination.



Strategy Update in Defence.

Speaker: Pirro Vengu, Minister of Defence, Albania

Moderator: Ieva Ilves, Advisor on Cybersecurity and Digital Policy, Ukraine/Latvia

Cyber defense has moved to the core of national security thinking in Albania, particularly following major cyber incidents in 2022. Pirro Vengu emphasized that cybersecurity could no longer be treated as a secondary or “hybrid” issue, but had to be fully integrated into military doctrine, investment, and training. In response to earlier vulnerabilities, Albania adopted a more centralized and top-down approach to cyber defense, particularly within the military, while maintaining a more flexible and innovation-friendly environment in the civilian sector. Alongside, he stressed that governments had to ensure that operators of critical infrastructure invested adequately in cybersecurity, supported by clear institutional frameworks.

Pirro Vengu also highlighted the growing importance of AI, both as a tool and as a potential threat. As AI increasingly benefits defenders and attackers in the cyber domain, Albania had chosen to actively embrace and institutionalize its use, including providing AI tools to public officials and exploring elements of sovereign AI capabilities. He noted that while innovation today was largely driven by the private sector, cyber and AI had to be treated as core defense issues. Drawing lessons from Ukraine, Vengu emphasized the importance of learning from real-world experience, while also underlining the need for sustained investment, stronger capabilities within NATO, and the continued development of technologically skilled personnel in the military.

Pirro Vengu:

“In the case of cyber defense we need to act top down otherwise it does not function. Otherwise we don’t have the necessary control.”



For Heaven’s Sake: Cyber Security in Space.

Speakers: Nina Armagno, Former Director of Staff of the U.S Space Force

Thierry Bauer, Director of Security and Cyber Defence, Eutelsat

Natalie Black, Group Director, Infrastructure and Connectivity, Ofcom

Declan Ganley, Chairman and CEO, Rivada Space Networks

Thomas Seifert, CFO Cloudflare, Chairman Supervisory Board, ICEYE

Moderator: Wolfgang Hackenberger, General Management, IABG

Space is increasingly emerging as a contested and strategically significant domain, closely intertwined with cybersecurity and global security dynamics. Nina Armagno stressed that alongside its civilian benefits, space was subject to growing geopolitical tensions, particularly from actors such as Russia and China. While the United States had long operated in this domain, she emphasized that the focus had now shifted toward building more resilient architectures and strengthening both defensive and offensive capabilities. Crucially, aging satellite infrastructure remained a key vulnerability, as many systems underpinning essential services on Earth remained insufficiently protected against modern cyber threats.

The role of satellite systems in ensuring connectivity and operational continuity was another key point of discussion. Declan Ganley outlined efforts to develop independent space-based networks capable of maintaining communications even if terrestrial internet infrastructure was disrupted. Moreover, Thomas Seifert highlighted how advances in satellite deployment had transformed their function, enabling near real-time observation and significantly enhancing military and intelligence capabilities. These developments, he noted, had already tangible impacts in ongoing conflicts, where space-based assets directly influenced outcomes on the ground.

Alongside these developments, speakers emphasized the growing complexity of governing this domain. Exemplifying these challenges, Natalie Black pointed to the challenge regulators faced in balancing innovation and security, particularly given the speed of technological change and the need for international coordination. In a similar vein, Thierry Bauer highlighted the dual-use nature of space infrastructure, stressing the importance of closer cooperation between commercial providers and defense actors to ensure resilience.

Against this backdrop, concerns about the lack of established norms and communication channels were raised. Armagno warned that the absence of clear rules, particularly in interactions with strategic competitors, increased the risk of conflict escalation. Overall, the discussion made clear that securing space required sustained investment, stronger cooperation, and a more strategic approach to managing an increasingly critical domain.



SPOT-ON: **Never Walk Alone! Management Priorities in 2026.**

Speakers: **Fiona van Echelpoel**, Deputy Director General, Market Infrastructure and Payments, ECB
Rick Driggers, Managing Director, Cyber Security Lead, Accenture
Johan Gerber, EVP, Head of Security Solutions, Mastercard

Moderator: **John Miller**, Information Technology Industry Council

AI is rapidly reshaping both cyber threats and defense strategies, with speakers highlighting its dual-use nature. From this perspective, Rick Driggers emphasized that cybercriminals were increasingly industrializing their operations using AI, lowering barriers to entry and scaling attacks, particularly in areas such as phishing. In response, organizations had to similarly “industrialize” cyber defense, while remaining realistic about AI’s limitations, as it cannot replace human judgment. Fiona van Echelpoel further noted that a large share of cyberattacks was now AI-driven, underscoring the importance of governance and workforce training. Moreover, Johan Gerber pointed to the growing challenge of distinguishing between human and machine actors, stressing the importance of maintaining trust across increasingly complex systems.

Speakers stressed that managing AI risks required clear governance and oversight structures. Johan Gerber warned that AI systems could be manipulated, making it essential to monitor both inputs and outputs, while Rick Driggers highlighted the importance of clearly defining authority and identity in AI systems. At the same time, organizations had to address the cultural dimension of AI adoption, ensuring that employees are equipped with the necessary skills and understanding. Without these adjustments, the rapid deployment of AI could introduce new vulnerabilities rather than mitigate existing ones.

The discussion also addressed broader systemic challenges, including the implications of quantum technologies and the need to secure critical infrastructure. Fiona van Echelpoel emphasized the importance of protecting financial systems, including payment infrastructures and initiatives such as the digital euro, from the outset.

Across the panel, speakers underlined the importance of partnerships, information sharing, and investment in people, stressing that effective cybersecurity depended not only on technology but also on collaboration and organizational readiness.



PANEL 5: **AI is Here to Stay! What Now?**

Speakers: **Bruce Schneier**, Lecturer and Author, Harvard University
Antti Koskela, President and CEO, WithSecure
Jacob N. Shapiro, Princeton University
Drew Bagley, VP, Chief Privacy Officer, CrowdStrike

Moderator: **Nicole Tisdale**, Aspen Institute

The panel explored the transformative impact of AI on cybersecurity, highlighting both its potential and the risks it introduces. In this context, Drew Bagley described AI as an accelerant that enabled adversaries to scale operations, identify valuable data more efficiently, and exploit vulnerabilities that would otherwise remain hidden. He also warned that the rapid and often unstructured integration of AI into technology stacks created additional attack surfaces. Antti Koskela, for his part, emphasized that while AI offered opportunities for improved security, most European companies, particularly small and medium-sized enterprises, lacked the internal capabilities to fully leverage these tools and had to rely on external providers.

A central theme of the discussion was the structural challenge of adapting security approaches to this evolving landscape. From a broader perspective, Jacob Shapiro noted that cybersecurity decision-making often relied too heavily on anecdotal evidence rather than systematic data analysis, while also highlighting a lack of effective communication across different stakeholder communities. Building on this, Bruce Schneier added that although AI tools were being widely adopted, the security of these systems remained insufficient, requiring new frameworks and approaches that were not yet fully developed. At the same time, speakers highlighted that the rapid deployment of AI was accelerating an already existing “arms race,” increasing the speed and scale of both offensive and defensive operations.

The panel also addressed how organizations and policy makers should respond to these developments. Looking ahead, Bruce Schneier pointed to the potential emergence of more adaptive, “self-healing” systems that could automatically address vulnerabilities, fundamentally changing how security is managed. Antti Koskela stressed the need for significant workforce reskilling as AI agents take over routine tasks, while Drew Bagley highlighted the importance of strong data governance as AI systems increasingly interact with one another. Finally, Jacob Shapiro emphasized the need for greater investment in public-interest tools to evaluate AI systems and to strengthen societal resilience against new forms of information manipulation and cyber-enabled influence operations.

The main takeaways from this panel were:

1. **AI is accelerating both cyber threats and defenses:** It enables attackers to scale operations while also offering new tools for detection and response.
2. **Current security approaches are not keeping pace:** Weak AI system security, fragmented knowledge-sharing, and anecdotal decision-making limit effective responses.
3. **Adapting to AI requires structural change:** This includes reskilling the workforce, strengthening data governance, and investing in new systems and public-interest capabilities.



TALKING HEADS:

Speakers: Sounil Yu, Chief AI Officer, Knostic
Igor Andriushchenko, CISO, Lovable
Nathaniel Gleicher, Head of Security Policy and Counter-Fraud, Meta

Moderator: Sergej Epp, CISO, Sysdig

The discussion focused on how AI is rapidly transforming the cybersecurity landscape, particularly by lowering barriers to software creation. Opening the discussion, Sergej Epp highlighted how AI enabled even non-technical users to build applications within hours, raising concerns about a massive expansion of potential vulnerabilities.

A central theme of the discussion was the difficulty of identifying and managing malicious intent in an AI-driven environment. Igor Andriushchenko argued that the key distinction between legitimate and malicious use rested in intent, but warned that platforms had to take responsibility by implementing safeguards to prevent misuse. Nathaniel Gleicher, on the other hand, argued that focusing solely on intent was insufficient, as the scale and automation enabled by AI fundamentally changed the threat landscape. He highlighted how AI introduced a new “actor” in cyber operations, enabling bad actors to scale activities such as disinformation, fraud, and identity manipulation in unprecedented ways. Building on this, Sounil Yu added that not all systems required the same level of security, emphasizing the distinction between verification (ensuring systems function correctly) and validation (ensuring they are used appropriately), the latter remaining a fundamentally human responsibility.

Overall, speakers agreed that AI represented both a major risk and an opportunity for cybersecurity. While attackers might benefit from increased scale and automation, defenders could also leverage these capabilities to improve detection and response. As highlighted by Nathaniel Gleicher, AI could help shift the balance by accelerating decision-making processes, while Sounil Yu stressed the need for new forms of deterrence and governance as AI systems evolve. In conclusion, Igor Andriushchenko argued that AI should be treated as a tool rather than an end in itself, requiring new skills, processes, and responsible implementation to ensure it strengthens rather than undermines security.



BREAKOUT 6: Guarding the Grid: Adapting Cybersecurity for Hybrid Threats to Critical Energy Infrastructure.

Speakers: Patricia Eke, Director, Cybersecurity and Emerging Tech Policy, Microsoft
 Gen. Christian Badia, (retired)
 Brig. Gen. Oleksandr Potii, Chairman of the State Service of Special Communications and Information Protection of Ukraine
 Maj. Gen. Karol Molenda, Commander of the Polish Cyber Command

Moderator: Maciej Bukowski, Director of the Energy and Resilience Program Casimir Pulaski Foundation

Protecting critical energy infrastructure has become a frontline challenge in an era of hybrid threats. Karol Molenda highlighted that Poland was among the most targeted countries globally, facing a sharp increase in attacks on infrastructure, including thousands of incidents requiring active response. He stressed that threats were often not isolated but part of coordinated campaigns, requiring a shift from a “need to know” to a “need to share” approach among trusted partners. More broadly, speakers emphasized that cyberattacks on energy systems were no longer purely technical disruptions but could have severe societal consequences, including loss of communication and public panic.

Operational readiness and coordination emerged as central challenges. Patricia Eke underscored that effective response depended on clear roles, pre-defined plans, and strong public-private cooperation, noting that the first hour of an incident was often decisive. Building basic competencies across institutions and ensuring that the right actors can be reached quickly were identified as critical for resilience. Drawing on NATO experience, Christian Badia emphasized that the speed and scale of current threats required a more proactive approach, moving beyond reactive defense toward stronger deterrence and integrated action across military and civilian domains.

Lessons from Ukraine further illustrated the realities of operating under sustained cyber pressure. Oleksandr Potii pointed to the importance of preparedness at all levels of society, including decentralized solutions such as backup energy sources and trained local response teams. At the same time, speakers highlighted structural vulnerabilities, particularly in legacy systems that were not designed with cybersecurity in mind. Addressing these risks required risk-based approaches, continuous adaptation, and closer cooperation with industry. Overall, the discussion made clear that strengthening energy security in the digital age depended on faster response mechanisms, improved coordination, and a more resilient infrastructure ecosystem.



BREAKOUT 7: Securing the Backbone of the Global Digital Economy: Subsea Cable Security.

Speakers: Despina Spanou, Deputy Director-General, DG CNECT, European Commission
Helen Popp, Ambassador-at-Large for Cyber Diplomacy, Government of Estonia
Sarah McComb, Principal, Global Network Planning & Acquisition, AWS
Markus Reinisch, Vice President, Public Policy Europe, Meta

Moderator: Alexander Botting, Senior Director, Global Security & Technology Strategy

Subsea cables form the physical backbone of the global digital economy, carrying around 95 percent of international data traffic and enabling everything from everyday communication to AI-driven services. Markus Reinisch emphasized that these infrastructures were critical not only for connectivity but also for economic growth and technological development, requiring significant long-term investment and maintenance. The speakers also emphasized that the 'cloud' was not abstract. Rather, it was a physical network of cables and data centers spreading across different locations. This made resilience and redundancy essential design principles.

The threat landscape surrounding subsea cables is complex but often misunderstood. Sarah McComb noted that while around 200 cable disruptions occurred annually, the vast majority were caused by natural events or human activity such as fishing, rather than deliberate sabotage. Physical attacks on cables were technically difficult and unlikely to yield direct access to data due to strong encryption. However, Helen Popp stressed that the strategic importance of these infrastructures made them a growing national security concern, particularly in regions such as the Baltic Sea, where cables often run alongside other critical infrastructure. The key risk were not isolated incidents but rather systemic vulnerabilities and the potential for coordinated disruptions.

Ensuring resilience therefore depended on a combination of policy, investment, and cooperation. Despina Spanou outlined a European approach based on three pillars – prevention, detection, and response – including risk assessments, improved repair capacity, and the development of regional cable hubs. Meanwhile, the speakers emphasized that public-private collaboration was indispensable, as governments alone lacked the expertise and operational capacity to manage these systems. Challenges remained, particularly in streamlining permitting processes, expanding repair capabilities, and addressing the aging fleet of cable repair ships. Overall, the discussion highlighted that strengthening subsea cable security required faster deployment, stronger partnerships, and a more coordinated strategic approach across Europe and beyond.



BREAKOUT 8: MCSC 2026 Guest Country: Kenya Insights from East Africa on Cyber Security Initiatives and Policies.

Members of Kenia Delegation include:

Dr James Kimuyu, Director NC4

Dr Josephine Mwanzia, Senior Director
Academic Affairs, Kenya School of Government

Dr Martin Koyabe, Senior Advisor,
Global Forum on Cyber Expertise GFCE Africa

John Mutunga, Founder CYBERPRO

Anne Macharia, ISACA Kenya Chapter

Margaret Mwinji, Mount Kenya University

Peter Wydler Orifah, NC4

Dr Katherine Getao, Former Minister
of Digital Affairs

Joy Kamau, Mount Kenya University

The session highlighted Kenya's emergence as a dynamic digital economy and a key entry point to the broader African market. James Kimuyu emphasized the country's strong demographic advantage, with a young, highly connected population and widespread use of digital technologies. Institutions such as the National Cyber Coordination Committee (NC4), bringing together multiple government entities, play a central role in strengthening national cybersecurity. At the same time, the speakers pointed to Kenya's growing investment in skills development, research, and education, particularly through initiatives that link academic institutions, government, and industry to better prepare the workforce for evolving cyber threats.

Looking beyond national efforts, the discussion underscored Africa's increasing relevance as a strategic partner in the global digital landscape. John Mutunga highlighted that engaging with Kenya provided access to a much larger regional market, positioning the country as a gateway to over 200 million people. Across the panel, the speakers stressed the importance of international collaboration, particularly between Europe and Africa, in areas such as cybersecurity policy, AI development, and innovation. Rather than viewing Africa solely as a recipient of support, the discussion emphasized its role as a source of innovation and growth, calling for stronger partnerships that combine European technological capabilities with African market opportunities and talent.



BREAKOUT 9: Digital Deterrence (U.S. and Europe).

Speakers: **Kemba Walden**, President, Paladin Global Institute
Yuliya Kazdobina, Head of the Ukrainian Foundation for Security Studies
Alexander Klimburg, Senior Fellow, The Hague Center for Strategic Studies
Andrea Rigoni, Managing Partner of Altirium; non-resident Senior Fellow, Atlantic Council

Moderators: **Lauryn Williams**, Deputy Director & Senior Fellow, Strategic Technologies Program, CSIS
Arthur de Liedekerke, Senior Director, Rasmussen Global

The session explored how deterrence is evolving in the cyber domain amid growing geopolitical tensions. Alexander Klimburg described deterrence as a layered concept, arguing that traditional models had proven insufficient, particularly in light of Russia's war against Ukraine. From a Ukrainian perspective, Yuliya Kazdobina reinforced that cyber and hybrid threats were now constant features of conflict, requiring a shift toward more active and sustained responses. Across the discussion, deterrence was framed less as preserving the status quo and more as actively shaping adversary behavior in a contested environment.

Strengthening European capabilities emerged as a central concern. Arthur de Liedekerke pointed to the need to move beyond compliance-driven approaches toward more proactive security strategies, while maintaining national sovereignty. At the same time, Lauryn Williams highlighted the importance of coordination at the European level, noting that fragmented structures continued to limit effectiveness. The discussion also touched on the idea of developing more integrated cyber capabilities, including closer alignment with NATO structures, while ensuring that political will and strategic clarity keep pace with technological change.

Public-private cooperation was identified as essential for making deterrence credible in practice. Kemba Walden emphasized that governments could not address cyber threats alone, as much of the relevant infrastructure and expertise resided in the private sector. Effective deterrence therefore depended on trusted partnerships, transparent information sharing, and clearly defined roles. Both Klimburg and de Liedekerke underscored that cyber deterrence had to be understood within the broader context of hybrid threats, where actions span multiple domains and require coordinated responses. Overall, the discussion highlighted that building credible digital deterrence required deeper transatlantic cooperation, stronger European integration, and a shift toward more proactive and coordinated action.



MCSC MEETS DEF CON



The joint session between MCSC and DEF CON opened with a reflection on the concept of “agency” in the digital age. Jeff Moss emphasized that individuals had to regain control over their digital identities, arguing that ownership of core elements such as domain names, email, and online presence was essential for autonomy. He also pointed to a structural imbalance in policy debates, where large technology companies dominated discussions while smaller actors, researchers, and civil society remained underrepresented. This lack of diverse perspectives, he suggested, weakened the quality of decision-making in an increasingly complex technological environment.

The first session focused on the development of agentic AI and the distribution of power within the ecosystem. Ariel Herbert-Voss, Daniel Cuthbert, and Yan Shoshitaishvili highlighted that AI capabilities were currently concentrated among a small number of major players, largely due to the high cost of compute and access to advanced hardware. While open and local models existed, they remained less capable, reinforcing global dependencies and raising concerns about strategic autonomy, particularly outside the United States.

Beyond structural issues, the discussion explored how AI is reshaping offensive and defensive dynamics in cybersecurity. Speakers noted that attackers often benefited from faster feedback loops, allowing them to iterate and improve more quickly than defenders, while organizations continued to struggle with securing complex infrastructures. Concurrently, AI significantly increased productivity, enabling faster research, analysis, and



automation. However, this also raised concerns about the erosion of foundational skills, as younger professionals relied more heavily on tools without fully understanding underlying systems.

This led to a broader reflection on the future workforce in cybersecurity. While AI could help bridge existing skill gaps, speakers stressed that human expertise remained indispensable, particularly for creativity, critical thinking, and system-level understanding. The idea of “self-healing systems” was discussed as a potential future development, with some suggesting that early versions are already emerging, although questions remained about their reliability and governance.

The second session shifted focus to network effects and their implications for digital agency. Meredith Whittaker and Jacob Braun emphasized that dominant platforms consolidated power by integrating multiple services, leaving users with limited alternatives, particularly small and medium-sized actors who could not afford to build independent infrastructure. These network effects were reinforced not only by technology, but by social behavior, making it difficult for new entrants or alternative systems to gain traction.

Closely linked to this was the issue of funding and sustainability. Louise Marie Hurel and Whittaker highlighted that many essential digital services, including secure communication tools, relied on underfunded or volunteer-

driven models, which limits their scalability and resilience. The discussion pointed to a structural gap: Neither large technology companies nor governments could fully fund these systems without creating dependencies, suggesting the need for new hybrid funding approaches that support open and independent infrastructures.

The final session examined in greater depth the limitations of current regulatory approaches to emerging technologies. Speakers including Hurel, Perry Adams, Jacob Braun, and Daniel Cuthbert argued that policy-making was often reactive, struggling to keep pace with rapid technological developments and uncertain risk landscapes. While some governments had experimented with strict regulatory models, there was broad skepticism about the feasibility and desirability of such approaches in open societies. The discussion highlighted tensions between ensuring safety, preserving innovation, and maintaining fundamental rights, particularly in areas such as content moderation, AI bias, and child protection.

Rather than relying on blunt instruments such as bans, the speakers called for more targeted and adaptive governance mechanisms. Cuthbert pointed to the need for practical tools, such as user-level controls or safeguards against specific harms like deepfakes, while Hurel emphasized the importance of understanding how AI systems function and how they are accessed by third parties. Moreover, Adams noted that outcomes were often shaped not only by regulation but also by the values and incentives of the companies developing these technologies. Across the discussion, a key challenge emerged: How to define desirable outcomes in a context where technological capabilities, societal expectations, and threat environments are all evolving simultaneously.

Ultimately, the session underscored that effective regulation cannot be developed in isolation. Speakers stressed the need to involve a broader range of stakeholders, including technical experts, civil society, and affected communities, in shaping governance frameworks, while also improving public understanding of these technologies. Without this approach, policy responses risked to remain either too slow or too simplistic to address the complexities of the digital landscape, the speakers warned.

DEF CON

is one of the world's largest and most influential hacker conferences, founded in 1993 by Jeff Moss. Held annually in Las Vegas, it brings together cybersecurity professionals, researchers, government representatives, industry leaders, and hackers from around the world. Originally created as an informal gathering of the hacking community, DEF CON has evolved into a major global platform for discussing cutting-edge developments in cybersecurity, digital rights, and emerging technologies.

A distinctive feature of DEF CON is its strong connection to civil society and independent researchers, providing perspectives that are often underrepresented in formal policy discussions. In recent years, the conference has increasingly engaged with policy makers and international organizations, serving as a bridge between technical communities and strategic debates on issues such as artificial intelligence, digital sovereignty, and cyber conflict.

To learn more about DEF CON, consult their conference report the Almanack:



OUTLOOK: The Next Cyber Front

Looking ahead, the cyber domain is entering a new phase characterized by technological acceleration and geopolitical competition. Artificial intelligence, in particular, is reshaping both the scale and nature of cyber threats, lowering barriers to entry while enabling more sophisticated and automated attacks. Meanwhile, critical infrastructure, from energy systems to subsea cables and space-based assets, is becoming increasingly interconnected, digitalized and, consequently, more exposed to hybrid threats. This evolving landscape suggests that future cyber risks will be less isolated incidents and more systemic in nature, with the potential to disrupt entire societies.

Against this backdrop, traditional approaches to cybersecurity are proving insufficient. The growing complexity of threats requires a shift from reactive defense to proactive resilience, combining technological innovation with strategic coordination. Concepts such as digital deterrence, cyber diplomacy, and public-private cooperation are likely to become even more central, as governments and industry must work together to anticipate and mitigate risks. In particular, the ability to share information, build trust, and coordinate responses across borders will be critical in managing threats that are inherently transnational.

At the same time, questions of sovereignty and control will continue to shape the cyber agenda. As dependence on global technology providers deepens, countries are increasingly seeking to balance openness with security, whether through supply chain diversification, investment in domestic capabilities, or regulatory frameworks. However, as the discussions throughout this report have shown, sovereignty cannot be achieved in isolation. Instead, it will depend on the ability to build resilient ecosystems that integrate national priorities with international cooperation.

Ultimately, the next cyber front will not be defined by technology alone, but by how effectively societies adapt to it. This includes investing in skills and workforce development, strengthening institutional capacities, and ensuring that governance frameworks keep pace with innovation. Concurrently, preserving trust between governments, industry, and citizens will be essential, as cybersecurity increasingly underpins economic stability, democratic resilience, and national security.

In this context, the challenge ahead is not only to respond to emerging threats, but to shape the digital environment in a way that is secure, inclusive, and aligned with democratic values.



We look forward to welcoming you to the upcoming

MCSC MUNICH CYBER SECURITY CONFERENCE **2027**

