Security Network Munich

CONFERENCE REPORT

MCSC MUNICH CYBER SECURITY CONFERENCE 2024

10TH ANNIVERSARY

www.security-network-munich.org

THIS CONFERENCE WAS ORGANISED BY:

Peter Moehring
Managing Director
Security Network
Munich

Lorenz Hoeppl
Security Network
Munich

Charlotte Kobel
Security Network
Munich

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

Marc Raimondi
Chief of Staff at
Silverado Policy
Accelerator

John Mengers
Founder and Executive
Director of C-Suite
Advisors

AUTHORS:

Stormy-Annika Mildner
Executive Director Aspen Institute Germany

In January 2021, Dr. Stormy-Annika Mildner (M.Sc.) became Director of the Aspen Institute Germany in Berlin, a renowned policy-oriented think tank 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). 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.

Vincent Tadday
Aspen Institute Germany

Vincent Tadday is a Program Assistant at the Aspen Institute Germany and part of the Institute's Digital Program, where he works on implementing high-level events and publication formats. Much of his writing and project work focuses on the intersection of geopolitics, trade, and technology policy. Vincent has professional experience in consulting, interest representation, journalism and field research. He holds a Bachelor's degree in Global Studies from Maastricht University and is currently pursuing a dual Master's degree in Public Policy at Sciences Po Paris and the Hertie School.

Driss Köhler
Aspen Institute Germany

Driss Köhler is Junior Program Officer at the Aspen Institute Germany and part of the Institute's Digital Program. Here, he is responsible for the conception, design, and implementation of the Institute's high-level events and publication formats on the most pressing digital topics. He primarily works and writes on geopolitics and geoeconomics, primarily focusing on transatlantic trade and technology relations. Before joining Aspen, Driss worked in the German Bundestag and at a consulting firm, focusing on public affairs mandates in EU regulation, digital, and cyber. Driss holds a Master's Degree in International Affairs from the Hertie School of Governance and a Bachelor's Degree in Public Governance from the University of Münster and the University of Twente.

Molly Hall
Aspen Institute Germany

Molly Hall is a Program Officer in the Digital Program the Aspen Institute Germany where she manages projects focused digital policy. She brings more than a decade of public affairs, strategic communications, and public policy experience to the role. Her research interests include cyber-security 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.

MCSC MUNICH CYBER SECURITY CONFERENCE 2024

Where to From Now?

Ways Forward out of The Cyber Conundrum

Patronage:

Bavarian Ministry of Economic Affairs, Regional Development and Energy

Supported by:

AIRBUS, paloalto NETWORKS, Giesecke+Devrient Creating Confidence, EY Building a better working world, accenture, BRUNSWICK, SIDLEY, Meta, aws, Google, TikTok, Infineon, SentinelOne, Recorded Future, WITH secure, Lenovo

Institutional Partners:

msc Munich Security Conference, CYBER READINESS INSTITUTE, Aspen Institute Germany, UNITED EUROPE competitive and diverse, Bundesamt für Sicherheit in der Informationstechnik, The Software Alliance BSA, ISF, CSSA Cyber Security Sharing & Analytics, bitkom, Charter of Trust, DsiN Deutschland sicher im Netz, invest in bavaria, BDI, ECS European Cyber Security Organisation, German Mittelstand, Keidanren Policy & Action, bayern innovativ Innovation leben., ZD.B Cyber-Security, ASPEN DIGITAL aspen institute, Alliance 4Europe, DGAP Advancing foreign policy. Since 1955., EnSure collaborative, DIGITALEUROPE

EXECUTIVE SUMMARY

With the Theme "Where to From Now? Ways Forward out of The Cyber Conundrum", the Munich Cyber Security Conference 2024 undertook the challenging task of navigating through the intricate maze of contemporary cyber threats and opportunities. This report encapsulates the essence of the discussions, findings, and recommendations that emerged from the conference.

Cybersecurity Must Adapt to a Changing Geopolitical Landscape: In 2024, the cybersecuri-ty landscape is marked by rapidly evolving technology and the escalating sophistication of cyber threats, influenced heavily by a turbulent geopolitical environment characterized by political un-certainty, social fragmentation, and rising global tensions. Notably, the Heidelberg Institute for International Conflict Research reports over 360 conflicts, with the majority involving violent dis-putes, underscoring the growing geopolitical instability. The evolution of cyber threats includes an alarming increase in politically motivated cyberattacks, with notable contributions from state-linked entities and non-state actors targeting essential infrastructures and political systems world-wide, aiming to destabilize and gain strategic advantages. This is part of a broader shift towards hybrid warfare, where cyber operations are integral to geopolitical strategies. The realm of cyberse-curity now also faces challenges from ransomware, supply chain vulnerabilities, and the use of AI and machine learning in cyberattacks, necessitating enhanced security measures and international cooperation.

Cyberspace is Transforming National Security and Defense: In this geopolitical environ-ment, the confluence of national security, defense, and cybersecurity is increasingly critical, as na-tions confront adversaries eager to exploit cyber domains to diminish military and technological strengths. The defense landscape has been profoundly reshaped by cyber threats, compelling na-tions to implement sophisticated cybersecurity measures to safeguard national assets and uphold strategic integrity. From July 2022 to June 2023, over 120 countries experienced nation-state cyberattacks. The need for a unified approach to cybersecurity has become more pronounced, with governmental agencies stressing the increased risks from the connectivity of numerous devices. This situation calls for robust protection of critical infrastructure and sensitive information, high-lighting the vital role of cybersecurity in safeguarding key sectors such as energy, transportation, and healthcare. To counter these threats, international collaboration and comprehensive cyberse-curity frameworks are becoming more essential. Organizations like NATO are enhancing global cyber resilience through collective defense strategies and partnerships, addressing the complexities posed by different cybersecurity laws and the disparity in technological capabilities among nations. Effective cybersecurity strategies now demand a proactive, cooperative approach that emphasizes ongoing threat assessment and comprehensive risk management. Integral to these strategies is the development of modern security architectures that include advanced preventative technologies and robust security principles. By fostering public-private cooperation and enhancing rapid re-sponse capabilities, nations and international partners can create a more secure cyber environment that effectively counters rising cyber threats and maintains the integrity of both national and inter-national security infrastructures.

Cyberattacks and Disinformation Threaten Electoral Integrity: In 2024, the role of cyberse-curity in safeguarding democracy is highlighted by the high stakes of multiple significant elections globally. As over two billion voters are expected to head to the polls, the integrity of these demo-cratic processes faces increasing threats from sophisticated cyberattacks and disinformation cam-paigns. These threats, which are only exacerbated by technological progress in AI, not only com-promise the security of electoral systems but also manipulate public opinion through strategically crafted misinformation, eroding trust in democratic institutions. Authoritarian regimes are intensi-fying their cyber operations to influence election outcomes and advance strategic geopolitical agendas. Amid these threats, there is a crucial need for a multifaceted approach to safeguard de-mocracy. This includes enhancing cybersecurity measures, implementing stringent regulations to ensure transparency in digital communications, promoting digital literacy to help the electorate discern credible information, and fostering international cooperation to combat cyber threats effec-tively. These efforts are supported by entities like the U.S. Cybersecurity and Infrastructure Securi-ty Agency (CISA) and the European Union Agency for Cybersecurity (ENISA), which provide critical resources and guidelines to protect elections and counter disinformation effectively. Addi-tionally, enhancing public-private partnerships and maintaining rigorous security protocols are vital in ensuring the resilience of electoral systems against the evolving landscape of cyber threats.

Cyber Resilience is the New Imperative: In 2024, the importance of cyber resilience has been firmly established as a critical component of strategic planning for organizations globally. Howev-er, a gap persists between the cyber resilience capabilities of large, resource-rich organizations and smaller enterprises, exacerbated by disparities in access to tools and skilled talent. Cyber resilience strategies now focus on maintaining operational continuity and quick recovery post-incidents, moving beyond traditional cybersecurity's preventative scope to embrace the inevitability of cyberattacks. This includes fostering a culture of resilience through regular training and robust in-cident management plans. Additionally, regulatory frameworks play a crucial role in ensuring or-ganizations meet minimum cybersecurity standards to protect consumer data and maintain public trust. Regulations like the EU's Network and Information Systems Directive and the Cyber Resili-ence Act set stringent cybersecurity obligations across various sectors and require robust measures across all stages of product development and service delivery. Emerging technologies such as AI and blockchain are innovatively utilized to enhance threat detection and response.

As digital threats evolve, so does the regulatory landscape, with new laws strengthening cybersecurity re-quirements across different regions and sectors, exemplifying the need for a balanced approach that fosters innovation while securing cyber ecosystems against increasingly sophisticated threats.

AI and Emerging Technologies are Revolutionizing Cybersecurity: The convergence of AI and cybersecurity is a critical evolution in the digital realm, bringing both enhanced defense mech-anisms and new threats. AI's role in cybersecurity is transformative, improving detection capabili-ties and enabling proactive defenses against cyber threats, while also providing cybercriminals with sophisticated tools for attacks. AI-driven technologies have significantly enhanced the efficiency of security measures, enabling the analysis and prioritization of threats in expansive network envi-ronments and automating network surveillance to detect anomalies. However, the same technolo-gies also empower cybercriminals to create more convincing deepfakes, crack passwords more ef-fectively, and automate personalized social engineering attacks at an unprecedented scale. AI's dual use presents a continuous arms race between cybersecurity professionals and cybercriminals, necessitating constant innovation and vigilance. Organizations and governments must navigate these dynamics carefully, harnessing AI's potential for defense while mitigating its risks to main-tain cyber resilience in an increasingly complex digital world.

Cyber Threats are a Systemic Risk to the Global Financial System: The digitalization of the financial sector has significantly increased its efficiency and reach but has also amplified its vul-nerability to cyber threats, which have evolved into systemic risks that could destabilize global financial systems. Now being the second most impacted sector by cyber threats, ransomware at-tacks, in particular, are increasing significantly year by year. For cyber criminals, the potential for severe disruptions makes the sector an attractive target. This rising trend emphasizes the critical need for a multifaceted strategic defense that includes preemptive actions, rigorous risk manage-ment, effective reporting mechanisms, and cooperative efforts. Regulatory bodies stress the im-portance of cybersecurity audits and the necessity for financial institutions to anticipate potential vulnerabilities, while international cooperation and sharing of threat intelligence are deemed cru-cial for defending against sophisticated cyber threats. The systemic risks are exacerbated by finan-cial firms' increasing reliance on third-party service providers, as seen in incidents where service disruptions were caused across numerous financial institutions simultaneously. Addressing these systemic vulnerabilities and ensuring robust defenses are essential for maintaining the stability and security of the financial sector in a highly interconnected and digital global landscape.

Cybersecurity through International Cooperation: The inherently borderless nature of cyber threats, coupled with their increasing sophistication, underscores the critical need for international cooperation in cybersecurity. This cooperation extends beyond traditional geopolitical boundaries, involving a diverse array of partners including countries, non-governmental organizations, and var-ious international entities. Successful cyber defense hinges on the collaborative efforts across these groups to share intelligence, strategies, and resources effectively. Central to this effort is the need to manage the complex web of cybersecurity regulations across different jurisdictions, which can pose significant compliance hurdles. Robust mechanisms for collaboration are essential, involving intra-state cooperation, multilateral agreements, international forums for consensus-building, and public-private partnerships that leverage both governmental insight and private sector innovation. However, challenges such as disparate legal frameworks, political tensions, varying levels of cyber-security readiness among nations, and the rapidly evolving nature of cyber threats complicate these cooperative endeavors. Operational coordination issues, including time zone differences and lan-guage barriers, further strain international cybersecurity efforts. Despite these obstacles, strategic international partnerships continue to enhance global cyber resilience, demonstrating a collective commitment to fortifying defenses against cyber threats and securing critical infrastructures and the global digital economy. This collaborative approach is essential for building a robust interna-tional cyber defense capable of responding effectively to the dynamic challenges posed by cyber threats.

As the landscape of cybersecurity in 2024 presents a complex array of challenges and opportuni-ties, the Munich Cyber Security Conference has laid the groundwork to navigate these endeavors, offering a platform for dialogue, knowledge exchange, and collaborative action in the face of ever-evolving cyber threats and highlighted the importance of principles of innovation, regulation, co-operation, and resilience guiding collective efforts to secure the digital world.

WELCOME

Claudia Eckert

Chairwoman of Security Network Munich (Munich)

In her welcoming remarks at the Munich Cyber Security Conference 2024, Claudia Eckert reflect-ed on the 10th anniversary of the MCSC and emphasized the importance of cooperation and coor-dination across different sectors in addressing cybersecurity challenges. She noted that despite sig-nificant efforts, too many activities remain uncoordinated. The conference theme, "Where to from now? Ways forward out of the cyber conundrum," underscored the need to share ideas and experi-ences as well as learn from each other in order to solve increasingly complex challenges. Key top-ics for discussion included the impact of deepfakes on democracy, the interplay between AI and security, and the role of regulation and standardization in either enabling or hindering progress. Eckert underlined her excitement about the diverse group of speakers and encouraged active en-gagement among attendees, as the conference thrived on such engagement.

GREETINGS

Georg Eisenreich

Bavarian State Minister of Justice (Munich)

In his opening remarks, Georg Eisenreich emphasized the growing importance of cybersecurity as digital threats become more severe and widespread. He highlighted how AI and ongoing conflicts, such as the war in Ukraine, are changing both defenses and attack methods in cyberspace, requir-ing increased vigilance and robust security measures. Eisenreich called for significant investment in cybersecurity and emphasized the need for international and cross-sector cooperation to address these evolving challenges. He emphasized that cybersecurity affected everyone, from nations to individuals, and that increased awareness and engagement were essential. Eisenreich concluded his remarks by urging all MCSC participants to redouble their efforts to combat cybercrime, stating that: "It is our duty to make the digital world as safe as possible."

10 YEARS MCSC

Ralf Wintergerst

Former Chair of Security Network Munich, President of Bitcom, Group CEO G+D (Munich)

Ralf Wintergerst's presentation at this year's MCSC highlighted the event's evolution from a mod-est gathering in 2014 to a major forum addressing critical cybersecurity issues. He reflected on the rapid advancement of technology, from the birth of the internet to the rise of artificial intelligence, and the challenges it has brought, such as misinformation and data misuse. The former Chair of the Security Network Munich emphasized the importance of international cooperation in overcoming cybersecurity threats, especially considering geopolitical tensions that can hinder global coopera-tion. He stressed that: "In a world where, especially in geopolitics, one's own advantage is valued more than cooperation in the affairs of mankind, we need to cooperate even more." Ralf Winter-gerst discussed the alignment between the MCSC and the MSC, noting that the growth of the MCSC over the past decade has been due in large part to an increased commitment to collective cybersecurity efforts.

OPENING KEYNOTE

Margaritis Schinas

Vice President of the EU Commission (Brussels)

Margaritis Schinas, Vice President of the EU Commission, highlighted the increasing sophistica-tion of cyberattacks, especially ransomware, and the critical vulnerabilities in sectors such as transport, energy, and healthcare. He warned that the cost of cybercrime could reach 23 trillion USD by 2027 and stressed the importance of the EU's legislative response. Schinas highlighted the need for cooperation between the EU, the United States, and NATO, as well as the dual role of AI as both a threat and a defensive tool. He stressed the urgency of addressing the cybersecurity skills gap, citing the EU Cybersecurity Skills Academy as an example of best practice. "We must remain constantly vigilant to changes and disruptions in cyberspace," he said, adding that defend-ers of free societies cannot allow foreign malicious actors to sow division and hatred in European democracies.

FIRESIDE CHAT

Anne Neuberger, Deputy Assistant to the President & Deputy National Security Advisor for Cyber & Emerging Technologies at the White House (Washington D.C.)

Moderator: **Dimitri Alperovitch,** Executive Chairman at Silverado Policy Accelerator (Washington D.C.)

During the fireside chat, Anne Neuberger highlighted the critical role of cybersecurity in national security, emphasizing the need for coordination across U.S. agencies. She addressed the global ransomware threat and the importance of the International Counter-Ransomware Initiative (CRI), which brings 56 countries together to share intelligence and develop common policies. In her conversation with Dimitri Alperovitch, Neuberger also stressed the need to secure telecom infrastruc-ture and reduce dependency on certain countries, particularly in light of ongoing threats like the Chinese-backed Volt Typhoon targeting critical infrastructure. "We need to translate the cyber measures to the operational measures and combine them with physical ones," she said, calling for new resilience measures to address evolving threats. Despite progress, the Neuberger emphasized that more frequent collaboration and partnerships were essential to keep pace with the fast-changing cyber landscape.

FIRST PANEL

Where to from now? A Cyber Strategy Update

Moderator: **Arthur de Liedekerke,** Senior Director for European Affairs at Rassmussen Global (Brussels)

Katherine Getao, Former CEO at ICT Authority of Kenya (Nairobi)

Nicola Hudson, Partner and Cybersecurity, Data & Privacy Global Lead at Brunswick Group (London)

Florent Kirchner, Head of National Cyber Security Strategy, Services of the Prime Minister (Paris)

Sami Khoury, Head of the Canadian Centre for Cyber Security (Ottawa)

Matthew Collins, Deputy National Security Advisor of the UK (London)

Jake Braun, Acting Principle Deputy National Cyber Director (Washington D.C.)

An international panel of global experts discussed the intersection of AI and cybersecurity, with each region highlighting its unique challenges and approaches and how national cyber strategies help them achieve their goals. Matthew Collins from the United Kingdom emphasized the need for rapid and sophisticated action to secure AI technologies through "cybersecurity by design," while his French colleague Florent Kirchner stressed the importance of focusing on achieving strategic autonomy in cyberspace. Sami Khoury, head of the Canadian Centre for Cyber Security, empha-sized the importance of public-private partnerships and the protection of critical infrastructure, stating that "partnership with business is key." He also pointed out that Canada was preparing to launch a new cybersecurity strategy. Meanwhile, Nicola Hudson warned that "businesses need to be better prepared for the organizational consequences of a cyberattack." Panelists emphasized the importance of global cooperation on cybersecurity, with Jake Braun noting that "we are only as secure as our allies," though obstacles such as antitrust laws and the complexity of information sharing remained. Katherine Getao, former CEO of the ICT Authority of Kenya, added that the scope of cybersecurity had to be broadened to include "all aspects of security," underscoring the need for extensive global cooperation.

KEYNOTE

Chris Wray

Director of the FBI (Washington D.C.)

In his keynote address, FBI Director Chris Wray emphasized the importance of global cooperation in combating increasingly sophisticated cyber threats. He pointed to the success of joint opera-tions, including the takedown of the Russian malware Snake and the dismantling of the Hive ran-somware network as evidence of how coordinated international action could neutralize major cyber threats. Wray pointed to China as the largest and most dangerous cyber adversary, combining hacking and espionage to target critical infrastructure around the world. He emphasized that de-spite the growing capabilities of adversaries, nations bound by the rule of law and shared values were collectively stronger. "We rely on our partners at home and abroad to get the job done," Wray said, noting that "none of us can go it alone" in a global cybersecurity battle where borders do not constrain malicious actors.

SECOND PANEL

Democracy under Stress: Collision of Elections and Disinformation

Moderator: **Vivian Schiller,** VP and Executive Director at the Aspen Institute (Washington D.C.)

Olga Belogolova, Director of the Emerging Technologies Imitative at John Hopkins University (Washington D.C.)

Sandra Joyce, VP Mandiant Intelligence at Google Cloud (Washington D.C.)

David Agranovich, Director for Global Threat Disruption at Meta (San Francisco)

Theo Bertram, Vice President, Government Relations and Public Policy for Europe at Tik Tok (London)

Nick Beim, Partner at Venrock (New York)

The second panel explored the growing challenge of protecting democratic processes amid rapid technological advancements. Panelists drew parallels between past technological disruptions, such as the printing press, and today's concerns about AI's potential role in disinformation. Sandra Joyce noted that while AI introduced new tools for manipulation, many of the tactics were famil-iar, explaining that "AI is just going to be another tool in this space." She also highlighted the dual nature of AI, which can either be used for beneficial purposes or be exploited by threat actors to create inauthentic content, raising the question, "how can governments prepare or inform their populations to understand this?". Nick Beim, Partner at U.S. venture capital firm Venrock, high-lighted the unprecedented speed at which AI was evolving, particularly in synthetic media, and warned that digital forensics to detect deep fakes were lagging behind AI advances. Despite the hype around AI, the panel agreed that the actual impact of AI on elections is still largely experi-mental, and traditional tactics remain central to defending democracies.

SPOT-ON

Limits of Control: An Intelligent View on Cyber

Moderator: **Christopher Ahlberg,** CEO of Recorded Future (Washington D.C.)
Sir Alex Younger, Former Chief of Secret Intelligence Service MI6 (London)
Sir Jeremy Fleming, Former Head of UK Intelligence Agency, GCHQ (London)

The session "Limits of Control: An Intelligent View on Cyber" moderated by Christopher Ahlberg, featured Sir Alex Younger and Sir Jeremy Fleming engaging in a thought-provoking discussion on modern intelligence and cyber threats. The two speakers argued that intelligence should be struc-tured around threats rather than traditional models, and that signals intelligence (SIGINT) and human intelligence (HUMINT) should complement one another rather than compete. Sir Jeremy Fleming emphasized the potential of technology for benefitting society and the importance of co-operation between nations and the private sector to address the challenges ahead, including the fragmentation of the internet and the evolving role of AI. Sir Alex Younger expressed concern about the widening technology skills gap, emphasizing the need for robust data management and international alliances to effectively address these issues. Both experts agreed on the critical need to integrate and ensure the quality of data used in AI systems to maintain security and trust.

THIRD PANEL

The Cyber Policy Dilemma: Regulation-Curse or Blessing for Business?

Moderator: **Siobhan Gorman,** Partner and Cybersecurity,
Data & Privacy Global Lead at Brunswick (Washington D.C.)

Claudia Plattner, President of the German Federal Office of Information Security (Bonn)

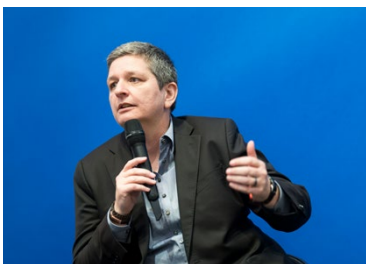
Julie Teigland, Managing Partner, EY EMEIA (London)

Siegfried Russwurm, President of the Federation of German Industries (Berlin)

Pascal Andrei, Chief Security Officer of Airbus (Toulouse)

Lorena Boix Alonso, Director for Digital Society,
Trust & Cybersecurity at European Commission (Brussels)

The third panel featured industry leaders and policy experts who discussed the delicate balance between business practices and regulatory measures in cybersecurity. While large organizations and critical infrastructure have improved their defenses, small and medium-sized businesses remain vulnerable. Claudia Plattner noted, "If every decision maker in a company knew what a good CISO knows, we wouldn't need regulation." Panelists emphasized that regulation was essential to protect critical infrastructure and correct market failures but must not stifle innovation. Siegfried Russwurm urged regulators to view regulation as helping businesses rather than an exercise in checking boxes. Lorena Boix Alonso added that the discussion about how to regulate cyberspace was just as important as what was regulated, and advocated working with industry to ensure that regulations helped rather than hindered technological progress. Pascal Andrei echoed this senti-ment, saying, "We need a framework for artificial intelligence, but please do not kill innovation." Ultimately, the panel agreed that a risk-based, collaborative approach was key to ensuring both security and continued innovation.



GUEST OF HONOR

Sviatlana Tsikhanouskaya, Opposition Leader Belarus (Minsk)
Moderator: **Maia Mazurkiewicz,** Co-Founder & Head of StratCom Alliance4Europe (Warsaw)

Belarusian opposition leader and guest of honor Sviatlana Tsikhanouskaya emphasized the vital role of civic awareness in safeguarding democratic values and national security. Drawing on her own experience under the regime of President Alexander Lukashenko, she highlighted how propaganda and disinformation was used to stifle dissent and manipulate public perception. "Countering propaganda in democratic countries and in dictatorships are two different things," Sviatlana Tsikhanouskaya noted, underscoring the unique challenges faced by those living under authoritari-an regimes. She called for greater support from technology companies to combat disinformation and promote media freedom, stressing that democracy had to remain resilient against both internal and external threats. Tsikhanouskaya concluded with a strong call for global solidarity and action to protect democratic principles in the face of evolving cyber and information warfare.

SECURITY NETWORK MUNICH
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 **www.security-network-munich.org**

Security Network Munich

KEYNOTE

Alejandro N. Mayorkas

U.S. Secretary of Homeland Security (Washington D.C.)

In his keynote address, U.S. Secretary of Homeland Security Alejandro N. Mayorkas discussed the evolution of cyberspace from its early vision as a free and open domain to the current reality of complex cyber threats. He noted that while the digital revolution initially promised an egalitarian world, increased connectivity had also brought increased risks, such as ransomware and cyberat-tacks. To address these challenges, Alejandro N. Mayorkas called for a new "cyber social com-pact" that balanced regulation and innovation, advocating a hybrid approach that combines man-datory security standards with voluntary commitments. "Like nuclear power or the automobile industry, a mandatory regulatory framework is needed to ensure its continued safety, trustworthi-ness, and usefulness," he said. A new cyber social compact would include core principles such as burden sharing, setting minimum security standards, and creating an agile regulatory framework to adapt to rapid technological change. Secretary Mayorkas stressed the urgency of government and industry working together to ensure a secure and resilient digital future.

VANTAGE POINT

Kazutaka Nakamizo

Deputy Director General of the NISC, Japan (Tokyo)

Kazutaka Nakamizo stressed the critical need to secure cyberspace, especially in light of upcoming global elections and heightened geopolitical tensions in East Asia. Citing recent cyber incidents in Japan, including attacks by China-backed and North Korean actors, he emphasized the importance of international cooperation to strengthen cybersecurity. Nakamizo highlighted Japan's proactive steps, including proposed legislation to improve public-private partnerships and dynamic vulnera-bility management systems. He noted that "international cooperation and public-private partner-ships are also key to securing emerging technologies such as AI," and reiterated Japan's commit-ment to secure-by-design principles. Looking ahead, Japan aimed to play a pivotal role in fostering a secure and resilient cyber environment in the Indo-Pacific region and beyond, he argued.

FOURTH PANEL

(IoT) Security by Design – Illusive, or will Norms and Standards Prevail?

Moderator: **Kiersten Todt,** CEO and Managing Partner at liberty Group Ventures, LLC (Washington D.C.)
Luis Jorge Romero, Director General of ETSI (Sophia Antipolis)
Katerina Megas, Cybersecurity for IoT Program Lead at NIST (Sterling)
Vincent Strubel, Director General of ANSSI (Paris)
Peter Stephens, Former Head of UK's "Secure by Design" Initiative (Paris)
Samantha Kight, Head of Industry Security at the GSMA (London)
Thomas Rosteck, Division President Connected Secure Systems at Infineon (Munich)

During the fourth panel, the importance of a "secure by design" approach was discussed. Secure by Design refers to security that is built into both software and hardware from the outset. Vincent Strubel, likened secure by design to world peace, noting, "You will find few people against it, but it does not tell you how to achieve it." The discussion also touched on the growing threat of na-tion-state and criminal actors targeting IoT devices and the need to raise security standards. Kate-rina Megas noted that "one size does not fit all" and emphasized the role of standards in address-ing diverse security needs. Thomas Rosteck advocated for efficient recognition of standards to avoid industry frustration with multiple certifications. Samantha Kight warned that "if your root of trust is not secure, then I question whether your supply chain is secure." The panel called for in-creased global cooperation, regulatory frameworks, and industry standards to incentivize better security practices and protect against evolving threats.

TALKING HEADS

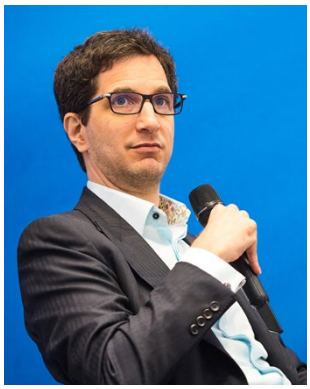
Limits of Control: An Intelligent View on Cyber

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

Kemba Walden, President of the Paladin Global Institute and Former Acting U.S. National Cyber Director (Washington D.C.)

Bruce Schneier, Fellow and Lecturer at Harvard Kennedy School (Cambridge, MA)

At this year's Talking Heads event at MCSC, Kemba Walden, President of Paladin Global Insti-tute and former Acting U.S. National Cyber Director, and Bruce Schneier, Lecturer at Harvard Kennedy School, highlighted how system complexity continues to outpace security measures. While decades of effort had made progress, fundamental issues such as password security remained due to the ever-increasing complexity of technology, both explained. Walden emphasized that se-curity by design had to start at the innovation stage, noting that regulators alone cannot ensure security without early intervention. Schneier emphasized the global impact of good standards, not-ing that "in a big enough market, they can move the planet." Moderator Jeff Moss added that cy-bersecurity was inherently a global issue, noting that "no one country is going to solve an internet problem." Walden and Schneier agreed to close the panel with a call for greater international coop-eration, shared responsibility, and emotional resilience in the face of future cybersecurity failures.



FIFTH PANEL

Intersection of AI and Cybersecurity.

Moderator: **Katie D'Hondt Brooks,** Director Global Cybersecurity Policy at Aspen Digital (Washington D.C.)
Koos Lodewijkx, CISO for IBM (Washington D.C.)
Heather Adkins, Vice President Security Engineering at Google (Mountain View)
Jason Ruger, CISO at Lenovo (Chicago)
Paul Vixie, VP and Deputy CISO at AWS (Redwood City)
Jonas Andrulis, Founder and CEO of Aleph Alpha (Heidelberg)

The fifth panel, featuring industry experts from various sectors, dispelled misconceptions about the role of AI in cybersecurity, explaining that AI was primarily used for augmentation rather than autonomous decision-making. While generative AI had gained attention, it did not radically change existing security strategies, the panelists pointed out. Heather Adkins emphasized the need for a secure by design, secure by default approach, especially when it came to securing supply chains. Paul Vixie meanwhile emphasized human responsibility: "It does not matter how good AI gets, the responsibility will always be with humans." Jonas Andrulis echoed this sentiment, arguing that humans had to remain in key decision-making roles because AI could not be the sole authority. Jason Ruger added that diversity was critical to addressing AI biases and increasing the reliability of its output. Throughout the discussion, it was emphasized that human oversight remained critical to the effective use of AI in cybersecurity.







CLOSING MODERATED KEYNOTE

Lisa Monaco, Deputy Attorney General of U.S. (Washington D.C.)
Moderator: **John Carlin,** Partner at Paul Weiss (Washington D.C.)

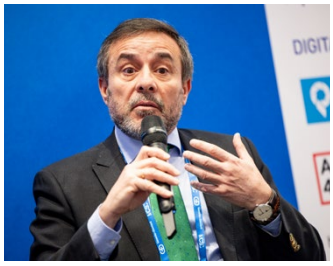
In her closing keynote, U.S. Deputy Attorney General Lisa Monaco emphasized the importance of focusing on victim assistance and proactively disrupting cyber threats. Some of the U.S. Depart-ment of Justice's significant accomplishments in recent years had included the infiltration and takedown of the Hive ransomware network, the takedown of state-sponsored malware from China and Russia, and the recovery of stolen funds. The Justice Department had also targeted the crypto-currency networks that enable ransomware, as evidenced by the actions taken against Binance. To address the misuse of AI, new initiatives aimed to enforce stricter penalties and the responsible use of AI. Lisa Monaco emphasized international cooperation, saying, "We are committed to working with our international partners to prosecute and hold individuals accountable."

SIXTH PANEL

Where the Money is – Insights from the Champions of Risk Management.

Moderator: **Wolfram Seidemann,** CEO at G+D Currency Technology (Munich)
Cheryl Venable, EVP, Chief of Payment Operations Federal Reserve Bank of Atlanta (Marietta)
Cheri McGuire, Chief Technology Officer at Swift (Virginia)
Ronald Green, Cybersecurity Fellow and Former Chief Security Officer at Mastercard (St. Louis)
Rafael Garcia Olivia, Deputy Director General in the Directorate general Information Systems at ECB (Frankfurt)
Sergej Epp, Chief Security Officer EMEA Central at Palo Alto Networks (Frankfurt)

Key trends and challenges in the payments sector were discussed in the sixth panel, highlighting the rise of instant payments as a critical tool for fast transactions in emergencies and e-commerce. Central banks and major financial institutions are increasingly focused on improving the efficiency and security of payment systems, with innovations such as central bank digital currencies (CBDCs) and blockchain technologies poised to transform the financial landscape. Ronald Green highlighted the rapid shift from traditional payments to digital and contactless payments and the importance of maintaining trust and security in these evolving systems. Sergej Epp underscored the complexity of securing financial systems, noting that "trust in money is very important, but the supply chain is very complex." Green added, "If people do not trust payments, they won't use them." Cybersecuri-ty experts warned of the growing risks associated with supply chain vulnerabilities, and the need for robust security as cloud computing and AI technologies are adopted across the financial sector. Cheryl Venable warned that poor risk management could lead to underinvestment in security, while Cheri McGuire stressed the need for new technologies to be both secure and interoperable to meet the G20's financial inclusion goals.



WORLD VIEW on Public-Private Partnerships

Akihiro Wada

Chair of Working Group at Committee on Cyber Security, Keidanren (Tokyo)

In his input statement, Akihiro Wada shared his perspective on cybersecurity issues, emphasizing strong public-private partnerships and cross-industry collaboration. In contrast to the top-down strategies seen in many Western countries, Japan had adopted a bottom-up model, with industry associations such as the Japanese Supply Chain Cyber Security Consortium (SC3) playing a key role, he explained. This approach had contributed to lower ransomware payment rates in Japan compared to other countries. Wada also emphasized the importance of international cooperation, pointing to Japan's recent memorandum of understanding with the United Kingdom as a model for global collaboration. He urged the cybersecurity community to "work together to make cyberspace a safe and secure domain by learning from each other's best practices."

SEVENTH PANEL

Connecting Dots in Cyber Defense.

Moderator: **David Lashway,** Partner at Sidley (Washington D.C.)
Emily Goldman, U.S. Cyber Command (Washington D.C.)
Manfred Boudreaux-Dehmer, NATO Chief Information Officer (Brussels)
Pekka Jokinen, Director at National Cyber Security Center Finland (Helsinki)
Michael Rogers, Admiral (ret.) U.S. Navy (New York)
Alexander Klimburg, Senior Fellow at The Hague Center for Strategic Studies (The Hague)

The final panel of the MCSC 2024 emphasized the need to gear up efforts in cybersecurity, using Ukraine's rapid cloud integration as a prime example of resilience in action. The discussion under-scored the importance of elevating cybersecurity responsibilities to senior leadership of organiza-tions, such as boards and CEOs, as well as adapting to evolving regulations. Emily Goldman not-ed that cyber was unique in that it created constant interaction with adversaries, directly impacting national power. Michael Rogers echoed the need for deeper integration, stating, "The future is in-tegration, it gives us speed." Pekka Jokinen praised collaborative counter-operations, such as in the case of the Snake and Volt Typhoon attacks, which highlighted the value of democratic rule-following in cybersecurity. Alexander Klimburg noted that adversaries often blured the lines be-tween cyber and disinformation, viewing them as a continuum. Manfred Boudreaux-Dehmer called for better regulation of basic security failures such as weak passwords.

We look forward to welcoming you to the upcoming

MCSC MUNICH CYBER SECURITY CONFERENCE 2025