@SN_Munich
#MCSC26

Security Network Munich

SECURITY NETWORK MUNICH
PRESENTS

MCSC
MUNICH CYBER SECURITY CONFERENCE 2026

12 / 13 February
Chamber of Commerce
Munich (IHK)

Command Control, Really?

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

Patronized by:

Bavarian Ministry of Economic Affairs, Regional Development and Energy

Supported by:

accenture · Allianz · BRUNSWICK · Google · Meta · schwarz digits · SAP · AIRBUS · aws · CLOUDFLARE · EY Building a better working world · Gieseckе+Devrient Creating Confidence · infineon · CROWDSTRIKE · Microsoft · paloalto NETWORKS · Recorded Future · SIEMENS · SIDLEY · WITH secure · TrendAI · Dataminr · eset Cybersecurity Progress. Protected. · NEC \Orchestrating a brighter world

Distinguished Guests,

Welcome to Munich, and welcome to this edition of MCSC, which aims to take a hard and honest look at the state of cybersecurity in 2026.

Geopolitical shifts, technological advancements, and the sheer scale and speed of cyber-related fraud and scams must be addressed with agility and resolve. Many governments have adapted their cyber security strategies to match the dynamics and dimensions of cyber -and increasingly- hybrid threats. This is an effort that, which seeks to change cyber economics from low cost and low risk for the offence and high cost with high risk for defence to a more balanced equation. Attackers should fear financial and legal consequences, more than they do now.

The conference - the title of which refers specifically to deterrence- should inspire and stimulate the discussions in support of these efforts.

For the first time, the MCSC welcomes a delegation from Kenya to join the forum. We are sure that insights and examples from different countries will help to foster not only exchange and collaboration but also serve as a source of inspiration and creativity in tackling the challenge of protecting and securing critical systems and services in business, government, and society. We have the foundation to do so; it is in your hands to make it tangible.

I wish you inspiring discussions.



Claudia Eckert

Chairwoman, Security Network Munich

Prof. Dr. Claudia Eckert is executive director of the Fraunhofer Institute for Applied and Integrated Security AISEC in Garching and professor at the Technical University of Munich, where she holds the Chair for IT Security in the Department of Informatics. Her research interests include the development of technologies to enhance the system and application security, the security of embedded systems, and the investigation of new techniques to increase the resilience and robustness of systems against attacks. As a member of various national and international industrial advisory boards and scientific committees, she advises companies, trade associations, and the public sector on all issues relating to IT security.

SECURITY NETWORK MUNICH

Europe's leading expert network for information security

The Security Network Munich (Sicherheitsnetzwerk München) is a non-profit association of leading players, organizations and research institutes in the field of information and cyber security founded in Munich. Members meet regularly to discuss pressing IT security challenges with corporates, government and research institutions. It also conveys 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. Aiming to promote cooperation and exchange among its members across different industries and academia, the Security Network Munich fosters innovation projects and education initiatives directed especially to students and young adults. It is committed to engage -together with its partners- in awareness and best practice campaigns with special emphasize on SMEs. For more information, please visit https://security-network-munich.org/.

Security Network Munich

EDITORIAL



Sami Khoury

Government of Canada Senior Official for Cyber Security, Communications Security Establishment

Confronting the Illusion of Deterrence in the Age of Relentless Cyber Threats

For years, the cyber security community has borrowed heavily from the vocabulary of traditional statecraft. We speak of signaling, thresholds, red lines, proportionality, and retaliation. At times, we reassured ourselves that the logic governing nuclear deterrence, risk of mutual assured destruction, or conventional escalation could be mapped onto cyberspace. But the accelerating trends shaping today's threat landscape have exposed the limits of that belief. We must now confront an uncomfortable reality: cyber deterrence, as traditionally conceived, is increasingly an illusion. Deterrence in cyberspace must evolve. It must be dynamic, multi-dimensional, and grounded in the recognition that no single measure - whether an active capability, a policy statement, or a defensive posture - can meaningfully alter adversary behavior on its own. Nations now pursue a blend of strengthened defences, public and sometimes joint attribution, and international coalition-building in the hope that, together, these efforts raise perceived risk and reduce the appetite for attack. This year's Munich Cyber Security Conference arrives at a moment of heightened geopolitical tension, rapidly advancing AI capabilities, expanding attack surfaces, and adversaries who operate without traditional constraints. Across the agenda - from economic risk and intelligence assessments to hybrid operations, space security, and transnational cybercrime - the message is clear: cyberspace does not behave according to the old rules.

Why Deterrence Fails in Cyberspace

Classical deterrence rests on three prerequisites: clear attribution, credible response, and meaningful consequences. Yet in cyberspace, all three are eroding. Attribution remains difficult and often contested. Credibility is undermined by the real risk of escalation or miscalculation. And consequences are rarely symmetrical; a ransomware gang can cripple a hospital with minimal resources, while a nation-state can impact critical infrastructure at negligible cost.

Cyberspace rewards anonymity, speed, and opportunism. Adversaries, whether states, criminal groups or hacktivist collectives need only persistence, creativity, and a willingness to exploit ambiguity. They thrive in a domain where the cost of attacks continues to fall while the cost of defence continues to rise. The fluidity of cyberspace, once celebrated as a driver of innovation, now serves as a shield for those who seek to undermine global stability.

Woven throughout the MCSC agenda is the idea of the dissolution of boundaries. Cybercrime crosses borders effortlessly. Intelligence operations blend with criminal infrastructures. Hybrid operations blur distinctions between war and peace, coercion and competition. AI compresses the timeline between detection and exploitation.

This asymmetry is visible across all sectors: defence is an unending marathon, while offense often requires only a single well-timed sprint. In today's digital landscape, the classical model of deterrence - convincing an adversary that the price of action outweighs the benefit - loses much of its theoretical and practical force.

A Canadian perspective

Canada recognizes that classical cyber deterrence - rooted in retaliation and punitive capability - is insufficient in a domain where attribution is contested and adversaries range from sophisticated state actors to loosely affiliated criminal groups. Instead, Canada intends to deter cyber threat actors as part of its national cyber objectives within a broader framework focused on resilience, defence, international norms and partnerships. This framework also advances responsible state behavior and uses transparent public attribution to expose and delegitimize malicious activity.

On the domestic front, resilience must form the backbone of every modern cyber strategy. It assumes adversaries will penetrate systems and focus instead on limiting impact, accelerating recovery, and ensuring continuity of essential services.

International collaboration is equally essential since the threats we face are inherently transnational. No single nation - regardless of technological sophistication - can counter state-sponsored operations, cybercrime networks, and hybrid attacks alone.

True security is derived by combining these two pillars: domestic resilience working in concert with durable, trust-based partnerships. By embracing this model, we move from fragile dependence on outdated deterrence assumptions to a proactive posture capable of withstanding and adapting to an ever-evolving threat landscape.

Confronting Reality, Together

As we open the Munich Cyber Security Conference, we do so with clarity rather than complacency. Classical cyber deterrence has not kept pace with today's threat environment. The illusion of deterrence may be comforting, but it is no longer sustainable. Recognizing this is not an admission of defeat - it is an invitation to adopt strategies grounded in realism.

Going forward, cyber deterrence must function as a continuous effort to manage and mitigate cyber risks. Its evolution is grounded in adaptation, adjusting strategies in response to each major incident and each new adversary tactic. In cyberspace, deterrence is at best partial and must be reinforced by robust defence and resilience.

By strengthening international collaboration and investing in domestic resilience, we prepare ourselves for the realities of an increasingly contested digital world. Every participant in this conference plays a role in shaping that transition and, in doing so, we protect the digital world we share.

IMPRINT

Publisher:
Security Network Munich

Layout:
Zeilbeck Design Company

© Security Network Munich, 2026
All rights reserved

Program Draft: Munich Cyber Security Conference (MCSC) 2026

THURSDAY, FEBRUARY 12TH

1:30–1:35 p.m.	**Welcome**	**Claudia Eckert** Chairwoman, Security Network Munich
1:35–1:55 p.m.	**Fireside:**	**Sean Cairncross** National Cyber Director, *in conversation with* **David Lashway**, Sidley
1:55–2:35 p.m.	**Panel 1:** Economies under Risk: What are we talking about? **Moderator: Barnabás Ferenczi** International Bankers Forum	**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
2:35–2:45 p.m.	**Strategy Update from Japan:**	**Yoichi Iida** National Cyber Director, Japan
2:45–3:05 p.m.	**Intelligence View:** Cyber Space, the Future Arena Of Political Conflicts? **Moderator: Paddy McGuiness** Brunswick Group	**Dag Baehr** Vice President, Federal Intelligence Service (BND), Germany **Paul M. Nakasone** Former NSA Director
3:05–3:25 p.m.	**Transatlantic View:** Overcoming Borders- Disrupting Cyber Crime **Moderator: Carsten Meywirth** Director Cybercrime, German Federal Police Office	**Catherine De Bolle** Executive Director, Europol **Andrew Bailey** Deputy Director, FBI
3:25–3:50 p.m.	**BREAK**	
3:50–4:40 p.m.	**Panel 2:** Offensive Defense: Legal Conundrum? **Moderator: Marc Raimondi** Silverado	**Florian Schütz** Director, NCSC, Switzerland **Thomas Goger** Chief Public Prosecutor, Bavarian Cybercrime Prosecution Office **Brett Leatherman** Director, FBI Cyber Group **Sandra Joyce** VP Threat Intelligence Group, Google
4:40–5:00 p.m.	**Executive View:** **Moderator: Alexander Schellong** Executive Management Board, Schwarz Digits	**Tom Leighton** Co-Founder and CEO of Akamai **Tomer Weingarten** Co-Founder and CEO of SentinelOne
5:00–5:40 p.m.	**Spot-On:** (Re)Interpreting (Cyber)Risk. **Moderator: Geoff Brown** CEO Silobreaker	**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

5:40 – 5:50 p.m.	**Keynote:** Responding to the Current Threat Landscape.	**Lisa Gustafsson** Director of Foreign Intelligence and Cyber at the Swedish Ministry of Defence
5:50 – 6:20 p.m.	**BREAK**	
6:20 – 7:00 p.m.	**Panel 3:** Risk Management Reset: Change of Mindset? **Moderator: Kiersten Todt** SVP Cybersecurity, Mastercard	**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
7:00 – 7:45 p.m.	**Panel 4:** Standing On The Shoulders of (Tech) Giants: Trust or Dare? **Moderator:** **Gabriel von Mitschke-Collande** Group CDO Giesecke+Devrient	**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
7:45 – 7:50 p.m.	**Greeting State Secretary**	**Tobias Gotthardt** Bavarian Ministry of Economic Affairs
7:50 p.m.	**Dinner Reception**	

INSTITUTIONAL PARTNERS:

Program Draft: Munich Cyber Security Conference (MCSC) 2026

FRIDAY, FEBRUARY 13TH

8:30–8:50 a.m.	**The Morning Brief with**	**Kaupo Rosin** Head of Intelligence Service, Estonia *in conversation with* **Oliver Rolofs**, Co-Founder, MCSC, Managing Partner, COMMVISORY
8:50–9:00 a.m.	**Vantage Point:**	**Josephine Mwanzia** Senior Director Academic Affairs, Kenya School of Government, on Capacity Building in Public Administration
9:00–9:10 a.m.	**The World's largest Honeypot:** Lessons learnt from the Taiwan Cyber Battlefield	**Yuh-Jye Lee** Senior Advisor, National Security Council, Taiwan
9:10–9:50 a.m.	**Across Borders:** Cyber Diplomacy Needed More than Ever! **Moderator: Katherine Getao** Cyber Ambassador and former Minister of Digital Affairs, Kenya	**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
9:50–10:00 a.m.	**Keynote:**	**Radmila Shekerinska** Deputy Secretary General NATO
10:00–10:15 a.m.	**Keynote:**	**Henna Virkkunen** Executive Vice-President, European Commission
10:15–10:45 a.m.	**Command Control, really?** Hybrid operations on the Rise! **Moderator: Chris Painter** Former US Diplomat	**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
10:45–11:00 a.m.	**BREAK**	
11:00–11:15 a.m.	**Strategy Update in Defence** **Moderator: Ieva Ilves** Advisor on Cybersecurity and Digital Policy, Ukraine/Latvia	**Pirro Vengu** Minister of Defence, Albania
11:15–12:00 p.m.	**For Heaven´s Sake:** Cyber Security in Space. **Moderator: Wolfgang Hackenberg** General Management, IABG	**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

12:00–12:30 p.m.	**Spot-On:** Never Walk Alone! Management Priorities in 2026. **Moderator: John Miller** Information Technology Industry Council	**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
12:30–1:10 p.m.	**Panel 5:** AI is here to stay! What now? **Moderator: Nicole Tisdale** Aspen Institute	**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
1:10–2:00 p.m.	**LUNCH BREAK**	
2:00–2:30 p.m.	**Talking Heads:** **Moderator: Sergej Epp** CISO, Sysdig	**Sounil Yu** Chief AI Officer, Knostic **Igor Andriushchenko** CISO, Lovable **Nathaniel Gleicher** Head of Security Policy and Counter-Fraud, Meta

MCSC meets DEF CON

LINE-UP: Jeff Moss (Founder DEF CON), Ariel Herbert-Voss (RunSybil), Louise Marie Hurel (RUSI), Daniel Cuthbert (Grupo Santander), Runa Sandvik (Founder Granitt), Yan Shoshitaishvili (Arizona State University), Meredith Whitakker (President Signal), Perry Adams (Dartmouth ISTS), Jacob Braun (University of Chicago)

2:30–2:35 p.m.	**Prelude:** Setting the scene	**Jeff Moss** Founder of DEF CON
2:35–4:45 p.m.	**DEF CON Sessions on Agency:** Being in control of our personal information and helping others be in control of theirs. **Moderator: Jeff Moss** Founder of DEF CON	**Session A** Agentic AI, Automation, Offence, and Agency: A conversation about the state of the art of AI offence and defence. Exploit development, and how companies and governments will have to adapt. **Session B** Network effects and the high cost of switching is why we can´t have nice things: Giant companies are in a good position to sort things to their advantage, but what about civil society, individuals, at risk communities and others? Let´s talk about what researchers, civil society and individuals do to increase their technical agency. **Session C** "Regulate the outcome" Why has policy failed to address the risks posed by AI and other next generation technology like global internet space connectivity in a winner takes all the environment?
4:45 p.m.	**End**	

Program Draft: Munich Cyber Security Conference 2026 – Track 2 (Breakouts)

THURSDAY, FEBRUARY 12TH Location: **BOARD ROOM**, one floor above the **MAIN HALL**

2:10–2:40 p.m.	**BREAKOUT 1:** Tech Sovereignty and Trusted Technology - Two Sides of the Same Coin? **Moderator: John Higgins** Chair, International AI Governance Association	**John Miller** General Counsel and Senior Vice President of Policy, ITI **Despina Spanou** Deputy Director-General, DG CNECT, European Commission
2:40–3:00 p.m.	**BREAK**	
3:00–3:45 p.m.	**BREAKOUT 2:** A New Threat: Resisting Algorithmic Propaganda. **Moderator: Oliver Rolofs** Co-Founder, MCSC, Managing Director, Commvisory	**Andrius Kubilius** European Comissioner for Defence and Space **Mykolas Katkus** Founder, Repsense **Günther H. Oettinger** President, United Europe **Ghee Leng** Founder, Embedded LLM
3:45–3:50 p.m.	**BREAK**	
3:50–4:35 p.m.	**BREAKOUT 3:** Asian Perspectives in a Fragmenting Digital World: Tech Sovereignty and Data Security **Lead commentator:** **Noboru Nakatani** Corporate EVP & CSO, NEC	**Yuh-Jye Lee** Senior Advisor, National Security Council, Taiwan **Jeff Greene** Distinguished Fellow, Aspen Digital - Aspen Institute
4:35–4:45 p.m.	**BREAK**	
4:45–4:50 p.m.	**BREAKOUT 4:** MSC Startup Hub "A new hope for Cyber Sovereignty?"	**Philipp Gerbert** CEO, TUM Venture Labs
4:50–5:35 p.m.	**New threats:** (One) technology to solve them all? **Moderator: Sarah Theinert** TUM Venture Labs	**Pawel Rybczyk** CEO, Labyrinth **Ben Kliger** CEO, Zenity.AI **Torben Leowald** Clandestine Technologies **Kseniia Semenova** President, NAU
5:35–5:45 p.m.	**BREAK**	
5:45–6:30 p.m.	**BREAKOUT 5:** MSC Startup Hub. The scale awakens. From breakthrough to deployment - why Europe lacks cyber champions. **Moderator: Sarah Theinert** TUM Venture Labs	**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
6:30 p.m.	**END**	

FRIDAY, FEBRUARY 13TH

Location: **BOARD ROOM**, one floor above the **MAIN HALL**

9:00–9:50 a.m.	**BREAKOUT 6:** Guarding the Grid: Adapting Cybersecurity for Hybrid Threats to Critical Energy Infrastructure **Moderator: Maciej Bukowski** Director of the Energy and Resilience Program Casimir Pulaski Foundation	**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
9:50–10:00 a.m.	**BREAK**	
10:00–10:50 a.m.	**BREAKOUT 7:** Securing the Backbone of the Global Digital Economy: Subsea Cable Security **Moderator: Alexander Botting** Senior Director, Global Security & Technology Strategy	**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
10:50–11:00 a.m.	**BREAK**	
11:00–11:30 a.m.	**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 Katherine Getao**, Former Minister of Digital Affairs **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 **Joy Kamau**, Mount Kenya University
11:30–12:30 p.m.	**BREAKOUT 9:** Digital Deterrence (US and Europe) **Moderators: Lauryn Williams,** Deputy Director & Senior Fellow, Strategic Technologies Program, CSIS and **Arthur de Liedekerke,** Senior Director, Rasmussen Global	**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
12:30 p.m.	**END**	

BREAKOUT PARTNERS:

SPEAKERS



Sean Cairncross

U.S. National Cyber Director, The White House

Sean Cairncross was confirmed as the National Cyber Director by the United States Senate on August 2, 2025, and joins the White House as President Trump's principal advisor on national cybersecurity policy and strategy. Before leading the Office of the National Cyber Director, Mr. Cairncross served as the Chief Operating Officer for the Republican National Committee, overseeing operations during both the 2024 and 2016 presidential cycles. In 2019, he was appointed by President Trump and confirmed by the U.S. Senate as the Chief Executive Officer of the Millennium Challenge Corporation. Prior to this appointment, he served as Deputy Assistant to the President and Senior Advisor to the White House Chief of Staff. Previously, Mr. Cairncross was a partner at a nationally recognized election law firm. He has also served as Deputy Executive Director and General Counsel to the National Republican Senatorial Committee under Senator John Cornyn (R-TX) from 2009 to 2013 and as RNC Chief Counsel from 2007 to 2009. Mr. Cairncross began his career at Covington & Burling and holds a J.D. from the NYU School of Law, an M.Phil. from Cambridge University, and a B.A., summa cum laude, from American University.



Catherine De Bolle

Executive Director, Europol

Catherine De Bolle is the Executive Director of Europol, the European Union Agency for Law Enforcement Cooperation, which supports EU Member States in preventing and combating all forms of serious and organised crime, cybercrime and terrorism. She assumed this role in May 2018, bringing extensive leadership experience from national and international policing. Prior to joining Europol, Ms De Bolle served as General Commissioner of the Belgian Federal Police from 2012, overseeing nationwide law enforcement operations and strategic reform. Before her appointment at the federal level, she was Chief of Police of the city of Ninove. From November 2015 to November 2018, Ms De Bolle was a member of INTERPOL's Executive Committee. Her distinguished service has been recognised with several honours, most recently her appointment as Commandeur in the Order of Leopold, awarded by His Royal Majesty the King of Belgium.



Andrew Bailey

Deputy Director, Federal Bureau of Investigation

Andrew Bailey was appointed co-deputy director of the FBI in September 2025. Following the terrorist attacks of September 11, 2001, he volunteered for a combat arms branch of service then volunteered to deploy to Iraq, where he served as an armored cavalry scout platoon leader from 2005 to 2006. Upon his return to the United States, his unit moved, refit, and trained for a subsequent fifteen-month deployment to Iraq from 2007 to 2009. Mr. Bailey began his legal career as a special prosecutor in the Missouri Attorney General's Office and then as an assistant prosecuting attorney in Warren County, Missouri. He then joined the Missouri Department of Corrections as general counsel and later served Missouri Governor Mike Parson as his general counsel. Governor Parson then appointed him as Missouri's 44th attorney general, where he served for two years prior to winning election to a full term.

SPEAKERS



Yoichi Iida

National Cybersecurity Office, Japan

Mr. IIDA was appointed National Cyber Director and Deputy National Security Advisor on July 1, 2025, after serving as Deputy Chief Executive at the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Director-General for Economic Security at the Cabinet Office, several key positions in international trade and industrial policies at the Ministry of Economy, Trade and Industry (METI), including Director-General of the Trade and Economic Cooperation Bureau and Director-General of the Trade Control Department. He currently leads the National Cybersecurity Office, which formulates a national cybersecurity strategy and develops detailed rules of the Active Cyber Defense Act.



Dag Baehr

Vice President, Federal Intelligence Service (BND)

Dag Baehr has been Vice President of the Federal Intelligence Service (BND) since 2023. He has served in the German armed forces since 1985 and has held a variety of assignments in intelligence and operations, including positions at the Federal Ministry of Defence, with NATO, from 2013 to 2017 as commander of the Special Forces Command (KSK), and most recently as commander of the Reconnaissance and Effects Command (Kommando Aufklärung und Wirkung). Baehr spent roughly six years on overseas deployments, during which he repeatedly served as commander of a Special Operations Task Force and was also deployed to war and crisis zones.



Paul M Nakasone

Founding Director, Institute of National Security, Vanderbilt University

General Paul M. Nakasone, a retired U.S. Army four-star general, serves as the Founding Director of Vanderbilt University's Institute of National Security. From 2018 to 2024, General Nakasone led U.S. Cyber Command and the National Security Agency, overseeing national cyber defense and global signals intelligence operations. A career military leader with more than three decades of experience, he has commanded at all levels, with deployments to Iraq and Afghanistan, and has held key intelligence and joint staff roles. A recognized authority on cyber operations and national security, General Nakasone continues to advance dialogue and research on emerging global security challenges, inspiring innovation and leadership in this critical field.



Henna Virkkunen

Executive Vice-President, European Commission

As Executive Vice-President for Tech Sovereignty, Security and Democracy, Ms Henna Virkkunen is tasked with combatting the increasingly complex security threats facing the EU, whilst at the same time strengthening our external borders and our internal security. This goes hand in hand with her responsibility to ensure our freedoms, justice and democracy are strengthened too.Furthermore, she is responsible for the Digital and Frontier Technologies portfolio. This entails leading Europe's efforts in shaping a competitive, resilient and inclusive digital future and maintaining or attaining leadership in strategic digital technologies. Prior to joining the European Commission Ms Virkkunen served as a Member of the European Parliament for over ten years. As a Member of the Committee on Industry, Research and Energy her work focused on digitalisation, research and frontier technologies. Ms Virkkunen has held various ministerial positions in Finland, namely Minister of Transport and Local Government (2014), Minister of Public Administration and Local Government (2011-2014) as well as Minister of Education and Science (2008-2011).

SPEAKERS



David Lashway

Partner Sidley Austin LLP

David Lashway is a partner at Sidley Austin in Washington, D.C. where he leads the global cybersecurity, privacy, and national security practice. He is widely recognized as a leading adviser for crisis management, cybersecurity, data security incidents, misinformation, trade secret theft, and related investigation and litigation matters. With more than 25 years of experience, David has advised a diverse range of private and public organizations on material cybersecurity incidents across almost every critical infrastructure sector. He has significant experience in addressing election security and misinformation-related issues and was deeply involved in the investigations into the 2016 and 2020 actions targeting various U.S. political parties.



Juergen Reinhart

Chief Underwriter Cyber, Munich Re

Jürgen Reinhart studied mathematics at the Technical University Munich and made his PhD in aerospace engineering at the University of Federal Armed Forces, Neubiberg, where he has worked as an assistant professor. Jürgen has been working for Munich Re since 1996 in various positions. As Chief Underwriter Cyber he has been driving the cyber business at Munich Re globally in the last decade. His responsibilities include the definition and implementation of the global Munich Re cyber strategy as well as setting the underwriting standards for the group. He carries the risk management function for cyber and is responsible for the service provider network and partnerships with respect to cyber business. He is also Deputy Chief Underwriter for the Munich Re Group.



Jürgen Michels

Chief Economist, BayernLB

Dr Jürgen Michels has been Chief Economist and Head of Research at BayernLB in Munich since October 2013. Prior to joining BayernLB, he served as an economist in Citigroup's Investment & Research Analysis (CIRA) department in London from 2002 to 2013, and became chief euro-area economist in 2008. From 1997 to 2002 he worked at Sal. Oppenheim in Cologne, and from 1996 to 1997 at the Institute for International Economic Policy at the University of Bonn. Dr Michels studied economics at the University of Bonn. He was conferred his doctorate degree by the University of Frankfurt.



Livio Stracca

Deputy Director General, European Central Bank

Livio Stracca is the Deputy Director General Macroprudential Policy & Financial Stability at the European Central Bank (ECB) and an adjunct Professor at the University of Frankfurt J.-W. Goethe. In his previous experience at the ECB, he has held different roles in the monetary policy, economics and international relations areas. He actively participates in, or leads, several fora and committees at both European and international level. Livio has a PhD in Economics at the University of Leicester and a postgraduate degree in European Union Law at King's College London. He has published extensively in international macroeconomics, international finance, and monetary economics, and is the author of the books The Economics of Central Banking, published by Routledge, and Redefining the Monetary Standard in the Digital Age, published by Palgrave Macmillan. In the area of climate and sustainability, he is the Chair of the Climate Scenarios Workstream in the Network for Greening.

SPEAKERS



Molly Lesher

Head of Digital Connectivity, Economics & Society Division, OECD

Molly Lesher is the Head of the Digital Connectivity, Economics and Society Division in the OECD Directorate for Science, Technology and Innovation. She has responsibility for measurement and analysis of digital transformation and its impacts; connectivity infrastructure and services policy; cybersecurity; consumer policy; and semiconductors. She also leads the OECD Digital Economy and Society Outlook and cross-cutting work on the economic and societal implications of digital transformation. Since joining the OECD in 2005, Molly has held a range of senior positions in both the OECD Directorate for Science, Technology and Innovation and the Trade and Agriculture Directorate. She also held roles in the Research Department of the US Federal Reserve Bank and the private sector (Fidelity Investments).



Barnabas Ferenczi

Munich Representative, International Bankers Forum (IBF)

Barnabas Ferenczi has 20+ years of experience in the payments industry, combining regulatory expertise with in-depth knowledge of technology and business. Throughout his career, he has held various leadership positions and played a key role in advancing the payments sector, from the Hungarian central bank to Giesecke+Devrient (G+D), a global security technology leader. Active across several industry communities: International Bankers Forum, Bitkom, Payment Association EU and the Mobey Forum.



Paddy McGuinness

Senior Adviser, Brunswick Group

Paddy McGuinness advises businesses and governments globally on geopolitical, regulatory and technology risks. He is a Senior Advisor at Brunswick Group and a member of the Advisory Committee of the UK's Counter Terrorism Reinsurance body PoolRe. Previously Paddy was Intelligence Security and Resilience Adviser to successive British Prime Ministers overseeing National Risk Assessment and response and recovery from all hazards and threats including Terrorism, Cyber and action by Hostile States. He was SRO for the National Cyber Security Strategy and chaired the Investment Security Group. Paddy served in the UK's Foreign Service leading variously on Counter Terrorism, Cyber, the Middle East, Iran, and Counter Proliferation with postings in Yemen, UAE, Egypt and Italy.



Carsten Meywirth

Director Cybercrime, German Federal Police Office

Director at the Federal Criminal Police Office and Head of the Cybercrime Department Carsten Meywirth has been Head of the Cybercrime Department at the Federal Criminal Police Office in Wiesbaden since April 2020. After completing his police training with the Lower Saxony State Police, he joined the BKA in 1987, where he has held management positions in the areas of organized crime, information technology, and central administration over the past two decades.

SPEAKERS



Florian Schütz

Director, National Cyber Security Centre NCSC

As Director of the National Cyber Security Centre, Florian Schütz is responsible for coordinating the implementation of the Swiss cyberstrategy (NCS) and managing the Federal Office. He further acts as the contact person for the cantons, the economy, scientific communities and the population. Florian Schütz holds a Master's degree in Computer Science and a Master of Advanced Studies in Security Policy and Crisis Management from the ETH Zurich. He has over ten years of experience in the field of cybersecurity. Since January 1, 2022, Florian Schütz has also chaired the OECD Working Party on Digital Security (WPDS). This enables Switzerland to make a significant contribution to increasing security in the global digital space. In addition, international engagement is another important pillar in the implementation of the NCS.



Thomas Goger

Chief Public Prosecutor, Bavarian Cybercrime Prosecution Office

Thomas Goger has been co-leading the Bavarian Central Office for the Prosecution of Cybercrime (ZCB) since its founding in 2015. This office is one of the largest units in Europe dedicated to the prosecution of high-profile cyber cases, with currently 30 prosecutors and several IT specialists supporting them. Thomas Goger has worked as a local prosecutor and district judge earlier in his career. He has been called upon as adviser to ministries and parliament on various cybercrime related topics. In 2016, he was seconded to the INTERPOL Global Complex for Innovation in Singapore for a few months. He has appeared as a speaker at and facilitator of various international events ever since. He is author of various articles in law journals on asset recovery regarding cryptocurrencies, on CSAM investigations and on MLAT reform. He also is associated scientist with the research training group "Cybercrime & Forensic Computing" at the Friedrich-Alexander-University Erlangen-Nuremberg.



Brett Leatherman

Assistant Director, Federal Bureau of Investigation

Brett Leatherman is the Assistant Director of the FBI's Cyber Division. Under Presidential Policy Directive 41, the FBI is the lead cyber threat response agency for the U.S. Government, and in this role, Mr. Leatherman serves as the senior executive managing the FBI's strategy to impose cost on some of the most sophisticated cyber adversaries targeting US interests. Prior to this role, Mr. Leatherman held several key leadership roles within Cyber Division and the Dallas Division. Mr. Leatherman entered on duty as an FBI Special Agent in 2003. He first served in the Cleveland and Detroit field offices, while also serving as an FBI pilot and hostage negotiator. He graduated from Cornerstone University with a degree in Computer Information Systems and received a master's degree in Cybersecurity Risk Management from Georgetown University. Mr. Leatherman holds several widely recognized cyber certifications and speaks internationally on emerging national security and cyber threats.



Sandra Joyce

VP Threat Intelligence Group, Google

Sandra is a cybersecurity leader with 27 years of intelligence experience. She leads Google Threat Intelligence and joined Google in 2022, following Google's acquisition of Mandiant. Sandra is a U.S. Air Force Reserve officer, serving as a faculty member and on the Board of Visitors at the National Intelligence University. She is the chair of the Aspen Institute Cybersecurity Working Group, the strategic council of the Silverado Policy Accelerator, and the Institute for Security and Technology's Ransomware Task Force Steering Committee. Sandra also joined the Board of Directors at Crane NXT. Sandra is pursuing her PhD at Johns Hopkins University as an Alperovitch Institute Fellow. She has an MBA from MIT and holds four additional master's degrees in cyber-policy, international affairs, science and technology intelligence, and military operational art and science. Sandra speaks English, Spanish, and German and resides in Virginia.

SPEAKERS



Marc Raimondi

Chief of Staff, Silverado Policy Accelerator

Marc Raimondi is Chief of Staff to the Executive Chairman of the Silverado Policy Accelerator, a bipartisan Washington, DC–based think tank focused on national defense, emerging technologies, trade, and energy security. He is also founder of Lexington Strategies, advising clients on government relations and strategic communications across the national security and technology sectors, and co-organizes the Munich and Paris Cyber Summits. Previously, Marc spent more than seven years at the U.S. Department of Justice, leading communications for the National Security Division and serving as chief spokesman and senior advisor to Department leadership. He directed responses to major national security crises, including terrorism, cyberattacks, and espionage cases. From 2016 to 2018, he served at the White House National Security Council as Director of Strategic Communications. Marc has also held senior roles at L3Harris Technologies, the Department of Homeland Security, and the U.S. Army, where he began his career as an active-duty infantryman.



Tom Leighton

Co-Founder and CEO, Akamai Technologies

Dr. Tom Leighton co-founded Akamai Technologies in 1998 as a Chief Scientist, becoming CEO in 2013. Under his leadership, Akamai has evolved from a content delivery network (CDN) into the cybersecurity and cloud computing company that powers and protects business online. Dr. Leighton holds over 50 patents and has authored more than 100 research papers. His accolades include the Marconi Prize (2018), induction into the National Inventors Hall of Fame (2017), and a Technology & Engineering Lifetime Achievement Emmy Award (2024). A long advocate for STEM education, first as a mathematics professor at Massachusetts Institute of Technology (MIT) and now through his leadership at The Akamai Foundation, he is committed to advancing early STEM careers. Dr. Leighton graduated summa cum laude from Princeton University in 1978 with a B.S. in Electrical Engineering and Computer Science. Dr. Leighton received his Ph.D. in Applied Mathematics from MIT in 1981.



Alexander Schellong

Executive Management Board, Schwarz Digits

Dr. Alexander Schellong serves as a Member of the Executive Management Board at Schwarz Digits, the powerhouse technology ecosystem of the Schwarz Group. In this capacity, he spearheads the Institutes, Accelerators, and Security division, overseeing the strategic integration of emerging technologies and Cybersecurity for one of the world's largest retail conglomerates. His career includes leadership positions across the United States, Asia, Europe and the Middle East in technology, defense, consulting and outsourcing, providing him with a unique cross-cultural perspective on global markets. He studied and taught at Harvard, Stanford, the University of Tokyo, Tec de Monterrey and Goethe University Frankfurt. At the intersection of policy and technology, Dr. Schellong focuses on the secure digital transformation of complex organizations and supporting women in Cybersecurity with the annual non-profit event CYBERWOMEN. He is dedicated to building resilient infrastructures that allow both public institutions and private enterprises to thrive in an increasingly volatile digital landscape.

SPEAKERS



Christopher Ahlberg

Co-Founder, Recorded Future

Christopher Ahlberg is the co-founder of Recorded Future. Earlier he was President of the Spotfire Division of TIBCO. Christopher Ahlberg founded Spotfire based on his ground-breaking research on information visualisation. He has lectured, published and consulted for industry, military and intelligence communities on topics covering cyber security, computer science, psychology, linguistics, biology and chemistry. He was named among World's Top 100 Young Innovators by MIT Technology Review in 2002. He has a doctorate from Chalmers University of Technology and is a member of the Royal Swedish Academy of Engineering Sciences.



Miguel De Bruycker

Director-General, CCB - Centre for Cybersecurity Belgium

After completing his studies at the Royal Military Academy in Brussels, Miguel De Bruycker worked with the Security Incident Response Capability unit of the Belgian Ministry of Defence. In 2005, he wrote a doctoral thesis on cyber defence. He then joined the General Intelligence and Security Service, where he was responsible for establishing Belgium's first cyber defence unit. In 2012, he took the initiative to draft the first National Cybersecurity Strategy. On 17 August 2015, he founded the Centre for Cybersecurity Belgium, where he still serves as Director-General. Under his visionary leadership, this national centre has significantly strengthened Belgium's cybersecurity, making Belgium one of the least cyber-vulnerable countries in the EU.



Louise Marie Hurel

Senior Researcher, RUSI

Dr. Louise Marie Hurel is a researcher in the Royal United Services Institute's Cyber and Tech team, specialising in cyber diplomacy, tech supply chain security, cyber attribution, the role of cybersecurity companies in statecraft, and cyber capacity building. She leads RUSI's international work on state responsibility in cyberspace and directs the Institute's Partnership for Responsible Cyber Behaviour. Over the past decade, Louise has investigated how middle-ground states develop cyber capabilities and strategies to achieve strategic advantage in cyberspace. Her doctoral research at the London School of Economics and Political Science (LSE) examined the history of private authority and the political economy of private cybersecurity companies—exploring how the commercial sector shapes global cyber governance. Louise serves as Senior Associate Fellow at Virtual Routes, co-chairs the Global Forum on Cyber Expertise (GFCE) Strategic Steering Committee, sits on Brazil's National Cybersecurity Committee, and is a member of the United Nations Institute for Disarmament Research's Roundtable for AI, Security and Ethics (RAISE). In 2023, she was named a CIDOB-Santander 35 Under 35 Future Leader.



Alexander Fitzsimmons

Acting Under Secretary of Energy, U.S. Department of Energy

Alex Fitzsimmons serves as the Acting Under Secretary of Energy at the U.S. Department of Energy (DOE). Fitzsimmons concurrently serves as Director of the Office of Cybersecurity, Energy Security, & Emergency Response (CESER), where he leads DOE's mission to safeguard the nation's energy systems against evolving cyber & physical threats. Prior to his current roles, Fitzsimmons served as Chief of Staff to Secretary of Energy Chris Wright. He previously served as Head of Government Affairs at Sila Nanotechnologies and as Senior Director at ClearPath. From 2017-2020, he served as Deputy Assistant Secretary and Chief of Staff in DOE's Office of Energy Efficiency and Renewable Energy. Fitzsimmons holds a Bachelor of Arts in Political Science from The George Washington University and a Master of Science in Cybersecurity from the Georgia Institute of Technology.

SPEAKERS



Geoff Brown

CEO, Silobreaker

Geoff Brown is CEO of the intelligence technology company Silobreaker, a position building upon recent senior executive roles in ransomware response and commercial threat intelligence. Geoff's overall career includes 15 years of public service at U.S. Federal and Local levels, spanning operational and executive roles, including six years as the founding director of New York City's cybersecurity agency. Geoff was a visiting professor for national security, intelligence, and cyber studies at MIIS in Monterey, is associated with academic programs at NYU, was a founder of NYC based Cyber Critical Services & Infrastructure, and has contributed to non-profit work in the cybersecurity and intelligence spaces throughout his career, including association with the Aspen Institute since 2018, and as a member of the Aspen Cybersecurity Group since 2022.



Carl-Oskar Bohlin

Swedish Minister for Civil Defence

Carl Oskar Bohlin is the Swedish Minister for Civil Defence, serving under Prime Minister Ulf Kristersson since 2022. His responsibilities include leading and coordinating the strategic development of Sweden's civil defence, which spans all 12 sectors of society. The Swedish civil defence aims to maintain vital societal functions, funnel support to the military in times of armed conflict, and ensure the protection of the civilian population during such events. Additionally, the Minister's duties encompass cybersecurity policies and combating disinformation. Bohlin holds the first dedicated civil defence ministerial role since the end of the Second World War.



Lars König

Head of Detection & Response, Allianz | NetWatch

Lars König is the Head of Detection & Response at Allianz, where he directs a global operation detecting and responding to cyber threats across 72 countries. A pioneer in AI-driven defense, he and his team transformed the Allianz SOC from manual operations into a highly automated ecosystem capable of real-time threat response at scale. Besides his work at Allianz, Lars also founded NetWatch, a community-backed initiative monitoring 4.5 billion attacks annually and taking down approximately 100,000 abusive systems per year in collaboration with ISPs and law enforcement. A member of the Google and CrowdStrike Technical Advisory Boards, Lars is also a frequent speaker at industry landmarks including Google Cloud Next, FalCon, and 38C3, where he presents innovative and sometimes unconventional solutions that disrupt threats before they can cause harm.



Jonathon Ellison

Director National Resilience, NCSC, UK

Jonathon holds the position of Director for National Resilience. He formerly served as the interim Policy Director. In his current role, he leads the NCSC's initiatives to enhance cyber resilience throughout the UK, spanning government, critical national infrastructure, and organisations of all sizes across the economy. He is responsible for the NCSC's work to build resilience at scale, which includes the NCSC's Active Cyber Defence Programme. He also leads the NCSC's 'Future Tech' programme of work to deliver long term resilience through ensuring the security of the technology that underpins the country's cyber security.

SPEAKERS



Richard Watson

Global Cybersecurity Leader, EY

Richard Watson is EY's Global Cybersecurity Leader, with 30 years' experience in professional services and IT, specializing in cyber risk and cybersecurity. He leads EY's global cybersecurity practice of more than 18,000 professionals, driving growth, solutions, and AI investments while serving clients worldwide. Richard advises organizations on understanding and mitigating cyber risk, with expertise in cyber risk assessments, security monitoring technologies, privacy regulation, and cyber incident response. He has worked across industries with high intellectual property value, strong brand risk exposure, or critical dependence on digital ecosystems. A recognized cybersecurity leader, Richard regularly advises senior executives and boards and is frequently cited in the media. Originally from the UK, he is based in Sydney and operates globally.



Claudia Plattner

President of the BSI

Claudia Plattner has been the President of the German Federal Office for Information Security (BSI) since 1 July 2023. Claudia Plattner was born in Mainz in 1973. She has more than 20 years of experience in IT functions for companies and institutions. Most recently, she served as the Director General for Information Systems at the European Central Bank and previously held a senior position as Chief Information Officer (CIO) of DB Systel GmbH, the internal IT service provider of Deutsche Bahn. Claudia Plattner holds a degree in mathematics (TU Darmstadt) and a master's degree in applied mathematics from Tulane University (USA).



Kiersten Todt

SVP Cybersecurity, Mastercard

Kiersten Todt is Senior Vice President of Cybersecurity Partnership and Engagement at Mastercard. She oversees Mastercard's global engagements with government entities and partners, facilitating collaboration to address evolving cyber threats and to promote secure innovation. Most recently, she served as President of Wondros, a service-driven creative company that specializes in storytelling and strategic communications. Kiersten served as Chief of Staff of the Cybersecurity and Infrastructure Security Agency (CISA); her government service also includes serving as Executive Director of President Obama's bipartisan Commission on Enhancing National Cybersecurity and as a professional staff member in the U.S. Senate, where she co-drafted the legislation to create the Department of Homeland Security. Kiersten co-founded the Cyber Readiness Institute, a non-profit focused on small business cybersecurity and supply chain resilience, and served as CEO of Liberty Group Ventures, LLC. She is a strategic advisor to venture capital firms and serves on boards of technology companies.



Martin Merz

President SAP Sovereign Cloud, SAP SE

Martin Merz serves as President SAP Sovereign Cloud and is a member of SAP's Senior Executive Team. He also acts as SAP's Shareholder Representative for SAP NS2. Since October 2024, he has led the Sovereign Services & Delivery organization, heading a global team responsible for cloud delivery, strategy, and regulatory compliance for governments and highly regulated industries. With more than a decade at SAP, Martin is known for his deep expertise in security, risk management, and operating in sensitive environments. He previously led SAP's Government Security organization and coordinated company-wide efforts to safeguard SAP's global risk posture. Before joining SAP, Martin held senior leadership roles in the German Armed Forces and allied organizations. He holds a diploma in Social and Political Sciences from Bundeswehr University Munich, with additional studies in Business Administration and Risk Management.

SPEAKERS



Rolf Schumann

Co-CEO, Schwarz Digits

Schwarz Digits, the IT and digital division of Schwarz Group, provides sovereign digital services in cybersecurity, cloud, AI, communication and workplace that adhere to Germany's strict data protection standards. As Co-CEO, Rolf Schumann oversees digital activities including e-commerce, loyalty, and retail media, aiming to unify these into a seamless omnichannel strategy. With over 30 years of experience, Schumann is a prominent leader in technology and digital innovation. Before joining Schwarz Group, he served as General Manager at SAP, leading the Platform and Innovation unit, and previously held the role of CTO for Europe. His career also includes founding a cleantech startup and nine years at Siemens managing European data center operations and internet architecture.



Andrea Campora

ECSO Chairperson, Managing Director Leonardo Cyber & Security Solutions Division

Andrea Campora is ECSO Chairperson since October 2025 and Managing Director of Leonardo's Cyber & Security Solutions Division since 2023, where he leads the division's growth, innovation, and strategic positioning in trusted cybersecurity and AI-driven data valorization for Defense, Space, and strategic organizations. Among the initiators of ECSO, he focuses on strengthening Europe's leadership in cybersecurity and building a future-proof European digital ecosystem. With over 20 years at Leonardo and prior global executive roles at Dematic and Sopra Steria, he brings extensive experience in cybersecurity, digital transformation, and strategic leadership. Additional current assignments: Vice President of Confindustria Genova on digital transition; Member of the Board of Directors of Nuclitalia; Member of the Technical-Scientific Committee of the Italian National Cybersecurity Agency. He holds a degree in Physics, specializing in Electronics and Solid State and has followed Executive Leadership Programs at the Columbia University of NYC and INSEAD, Paris.



Amy Hogan-Burney

CVP Customer Security & Trust, Microsoft

Amy Hogan-Burney is Corporate Vice President and Deputy General Counsel in Corporate, External, and Legal Affairs at Microsoft, where she oversees the Customer Security and Trust (CST) organization. CST is a cross-disciplinary team working to advance customer trust through global cybersecurity policy, disruption of nation-state cyber and influence operations, combatting cybercrime, and supporting democratic institutions. CST manages Microsoft's U.S. government clearance and national security compliance and develops engineering solutions supporting law enforcement and national security efforts. AI is a core component of CST's work, accelerating policy, regulatory, detection, and disruption initiatives. Prior to leading CST, Amy headed Microsoft's Cybersecurity Policy and Protection team, played a key role in GDPR implementation, and managed the Law Enforcement and National Security team. Before Microsoft, she served as attorney at the U.S. Department of Justice, Federal Bureau of Investigation. She holds a B.S. in Biomedical Engineering and J.D. from The Catholic University of America.

SPEAKERS



Markéta Gregorová

Member of the European Parliament

Markéta Gregorová is a Czech Member of the European Parliament, representing the Czech Pirate Party. She has served in the European Parliament since 2019, where she focuses on cybersecurity, digital resilience, foreign interference, and the protection of democratic processes. In the current legislative term, she has been designated as lead negotiator for the revision of the EU Cybersecurity Act, shaping the Parliament's position on ICT supply chain security, the role of ENISA, and the strengthening of European cyber resilience. Within the European Parliament, she is a member of the Committee on Industry, Research and Energy, the Committee on Civil Liberties and the Committee on International Trade, and she has served on the Special Committee on Foreign Interference in all Democratic Processes in the European Union. Her work consistently emphasizes European digital sovereignty, transparency, and the protection of fundamental rights in the digital sphere.



Gabriel von Mitschke-Collande

Group CDO Giesecke+Devrient

Gabriel von Mitschke-Collande is a member of the Giesecke+Devrient (G+D) management board. As Group Chief Digital Officer (CDO), he is responsible for digitalization, IT, technologies, and innovation, as well as environmental, social, and corporate governance (ESG). He is also in charge for Group and information security, quality management, and G+D Ventures.Von Mitschke-Collande has successfully implemented digital transformation in various management positions. Most recently, he was CDO at BayWa AG in Munich. Since May 2024, he has been responsible for G+D's digital and ESG strategy as Group CDO. In addition, he has been a Board Member of the Security Network Munich since December 2025. Gabriel von Mitschke-Collande's academic journey includes studying management and technology at TU Munich. He further honed his skills with a master's degree, focusing on mechanical engineering, innovation, and entrepreneurship.



Tobias Gotthardt

State Secretary in the Bavarian Ministry of Economic Affairs, Regional Development and Energy

State Secretary in the Bavarian Ministry of Economic Affairs, Regional Development and Energy since November 8, 2023. Tobias Gotthardt was born on June 3, 1977 in Regensburg and grew up in Burglengenfeld and Kallmünz. After completing his high school education and studying political science in Regensburg and Freiburg, he initially worked as a parliamentary assistant and head of office in the European Parliament and the German Bundestag. After his election to the Bavarian State Parliament in 2018, he assumed the chairmanship of the Committee for Federal and European Affairs. In addition, in 2021, he was appointed as deputy and then acting chairman of the Committee of Education and Culture. At the same time, he was the federal, European, education and youth policy spokesman of the FREIE WÄHLER parliamentary group. After his re-election, Tobias Gotthardt was appointed State Secretary and member of the Bavarian State Government in 2023.

SPEAKERS



Matt Collins

UK Deputy National Security Advisor

Matt Collins - Deputy National Security Advisor- Intelligence, Defence and Security in the Cabinet Office. Matt has been in the Civil Service for 20 years, most recently in his role as Director for Intelligence, Technology and Security within the National Security Unit in the Cabinet Office. The extensive portfolio covered counter-terrorism and serious and organised crime, oversight of intelligence finance, critical and emerging technology and digital, Cyber, data and intelligence policy. He previously worked in the Office for Security and Counter Terrorism where he was responsible for the Prevent pillar of the UK counter-terrorism strategy and for targeted communication campaigns to prevent terrorism and serious and organised crime. He has worked internationally to tackle online harms, particularly to prevent terrorist's use of the internet.



Kaupo Rosin

Director General, Estonian Foreign Intelligence Service

Kaupo Rosin is the Director General of the Estonian Foreign Intelligence Service since 1 November 2022. Prior to that, he served twenty-seven years in the Estonian Defense Forces (EDF). His last post was as the Commander of Cyber Command, from where he retired with the rank of Colonel. From 2018 to 2022, he served as the Deputy Director of the Analysis Unit of the Joint Intelligence and Security Division at NATO Headquarters in Brussels, and before that as Commander of the Military Intelligence Centre of the EDF from 2012 to 2018. He has also held various positions in the General Staff of the EDF and the Intelligence Battalion. In 2005, he was deployed to Iraq and served at the Multi National Force-Iraq HQ. Mr. Rosin holds a M.B.A. in economics from the Universität Bundeswehr München and has completed the National General Staff Course of the Führungsakademie der Bundeswehr.



Oliver Rolofs

Co-Founder, MCSC, Managing Partner, COMMVISORY

Oliver Rolofs is Founder and Managing Partner of COMMVISORY, a Munich-based strategy strategic communications consultancy. He is also director of the Vienna based Austrian Institute for Strategic Studies and International Cooperation (AISSIC). Oliver looks back on a successful longstanding career in politics, business and communications, international conference organization and strategy consulting for political decision makers and business leaders. Prior to joining COMMVISORY he worked as Managing Partner of a strategy consultancy and earlier as a senior communications officer for the global consultancy firm Roland Berger. Earlier he was the longstanding Head of Communications for the internationally renowned Munich Security Conference where he also established the cybersecurity and energy security programs. Furthermore, he is co-founder of the annual Munich Cyber Security Conference (MCSC) and a regular moderator of events. He studied political science, international law and sociology and graduated with a master's degree from the Ludwig Maximilian University of Munich.

SPEAKERS



Josephine Mwanzia

Senior Director, Academic Affairs, Kenya School of Government

At the School, Dr. Josephine Mwanzia is responsible for development and implementation of training, research, policy advisory and technical support to bridge performance and service delivery gaps in Government, including integrating emerging technologies as a learning solution. Dr. Mwanzia is the current Chairperson of the Cyber Week Africa Conference that is convened annually in October. She is the author of Participatory Development in Kenya, which highlights inclusive decision making in public policy formulation and programming. Dr. Mwanzia has served at senior management positions in the Public Service of Kenya, with 35 years of practical experience in leadership and governance, education and training and policy formulation. She holds a Doctor of Philosophy in Education from Victoria University of Wellington, New Zealand, Master of Education Management from Universiti Brunei Darussalam and Bachelor of Education (Arts) from the University of Nairobi.



Yuh-Jye Lee

Senior Advisor, National Security Council, Taiwan

Dr. Lee is a leading expert in artificial intelligence and cybersecurity, currently serving as Senior Advisor to Taiwan's National Security Council. He received his Ph.D. in Computer Sciences from the University of Wisconsin–Madison in 2001 and has held academic and leadership roles at top institutions, including Academia Sinica and National Yang Ming Chiao Tung University. Dr. Lee's research focuses on the convergence of AI and national security, with interest in applications such as unmanned systems, C4ISR architectures, and decision support technologies. As the initiator of the Trustworthy AI Dialogue Engine (TAIDE)—Taiwan's sovereign large language model based on Meta's Llama—he plays a key role in advancing trustworthy and resilient AI infrastructures. He previously served as Deputy Executive Secretary at the National Science and Technology Council, helping shape Taiwan's science and technology strategy. Dr. Lee remains actively engaged in promoting AI applications that enhance national defense, strategic autonomy, and technological resilience.



Luca Tagliaretti

Executive Director, European Cybersecurity Competence Centre (ECCC)

Luca Tagliaretti is the Executive Director of the ECCC since February 2024. Prior to that he was Deputy Executive Director and Interim Executive Director of eu-LISA and before head of the International Anticounterfeit Deterrence Centre at the European Central Bank in Frankfurt am Main.



Felix Kroll

German Federal Foreign Office

Felix Kroll currently serves as Cyber Coordinator of the German Federal Foreign Office. Prior to this role, he led the Political Section at the German Permanent Mission to the UN in Geneva and served as Deputy Head of the Coordination Staff for Cyber Foreign Policy and Cyber Security. His career also includes positions with the German Permanent Mission to NATO in Brussels and at the German Embassy in Bamako. Additionally, he has worked in the Ministry's Division for Scientific Cooperation and held the role of Deputy Consul General at the German Consulate General in Mazar-e Sharif. Felix Kroll is a graduate of Eberhard Karls University in Tübingen and is a Fulbright alumnus.

SPEAKERS



Martin Koyabe

Senior Advisor, Global Forum on Cyber Expertise (GFCE) Africa

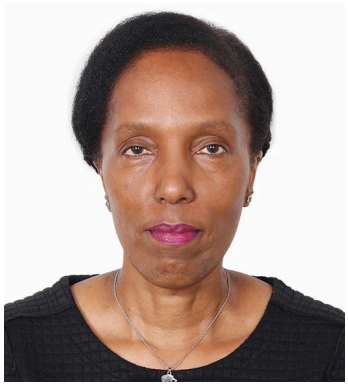
Dr Martin Koyabe has over 30 years of experience working on ICT deployment, innovation, research and development, policy, regulation, and legislation. He is a Senior Advisor at the Global Forum on Cyber Expertise (GFCE) Africa; and founder of MWK Consult a tech-startup on AI and Emerging Tech operating in Africa. He is currently leading a number of key Cyber initiatives and projects in Africa, including implementation of the Africa Agenda on Cyber Capacity Building (AA-CCB) with AUDA-NEPAD, KPMG-GFCE Technical Assistance (World Bank Funded) Project for Togo aimed at Enhancing Regional Cooperation for Cyber Resilience through the Centre for Coordination and Research in Cybersecurity (ACCRC); African Union (AU)-CSIRT/CERT Project (LuxDev Funded) to Secure Africa's digital Infrastructure, GFCE-AUDA_NEPAD Coordination Committee on Cyber Capacity Building (CCB) in Africa, and the AU-GFCE Collaboration Project (Bill & Melinda Gates Funded) to Enhance Cyber Capacity Building (CCB) and Cyber Resilience across all 55 Africa Union member states.



Anny Vu

Senior Bureau Official for the Bureau of Emerging Threats, U.S. Department of State

Anny Vu is the State Department Senior Bureau Official for the Bureau of Emerging Threats. A career member of the Senior Foreign Service, she served as Charge d'Affaires at U.S. Embassy Beijing. Her extensive experience includes roles as Senior Advisor to the Undersecretary for Political Affairs, Political Chief at the American Institute in Taiwan, Deputy China Coordinator, and a member of the Secretary's Policy Planning Staff. At the White House, Anny served as Special Assistant to the President and NSC Senior Director for International Organizations during President Trump's first term, along with multiple NSC roles covering Africa, UN, and China. She also served at the U.S. Mission to the UN, at U.S. Embassies Beijing and Paris, Secretary's Operations Center, and Bureaus of East Asian and Pacific Affairs and Western Hemisphere Affairs. A graduate of Johns Hopkins School of Advanced International Studies and UCLA, Anny speaks Mandarin, Vietnamese, Indonesian, and French.



Katherine Getao

Cyber Ambassador and former Minister of Digital Affairs, Kenya

Dr. Katherine W. Getao, EBS, is often dubbed an "ICT Elder" in Kenya, in recognition of her 40 years of service in the private sector, academia, diplomacy as well as senior government appointments. Dr. Getao currently executes consultancy assignments in the areas of Cyber Hygiene, Cyber Diplomacy and ICT Strategy and Governance. She has served as the Chief Executive Officer of the ICT Authority in Kenya, the ICT Secretary in the Office of the President and subsequently at the Ministry of ICT. Dr. Getao previously served as the Director of the School of Computing and Informatics at the University of Nairobi. She has represented Kenya on UN Governmental Committees and has also served on the boards of private companies and universities. Dr. Getao is passionate about public service transformation using ICTs and the creation of industries and career opportunities for young people in the ICT Sector.

SPEAKERS



Michael Vetter

Director-General and Chief Information Officer, German Armed Forces

Lieutenant General Michael Vetter is a senior leader of the German Armed Forces and a key figure within the German Federal Ministry of Defence, where he has played a central role in driving the Bundeswehr's large-scale IT and digital transformation. He has been responsible for modernizing mission-critical information systems across one of Europe's largest and most complex public-sector organizations, ensuring operational readiness, resilience, and security in an increasingly volatile geopolitical environment. He has overseen the alignment of digital capabilities across military branches, governmental stakeholders, and partners, with a strong focus on cybersecurity, sovereign IT infrastructure, and secure command-and-control systems. Drawing on decades of leadership experience, he brings deep expertise in change management, large-scale organizational transformation, and decision-making under high-stakes conditions.



Rob Magowan

Commander Cyber & Specialist Operations (Des.), UK Ministry of Defence

Rob Magowan joined the Royal Marines in 1989 after reading chemistry at Southampton university. His career to Lt Col included an operational tour of Northern Ireland, US Marine Corps staff college, the first deployment to Afghanistan post 9/11 and the invasion of Iraq in 2003. Subsequently, he worked in the Cabinet Office, the Foreign and Commonwealth Office and the Ministry of Defence, with a focus on intelligence. He commanded the Royal Marines 30 Commando Information Exploitation Group, redeploying to Afghanistan. As a Brigadier he spent a year in Kabul, was head of Royal Navy people policy and commanded the UK's Joint Forces Intelligence Group. As a Lieutenant General, he was deputy commander of the then UK Strategic Command and then head of capability for Defence. He will be appointed Commander Cyber & Specialist Operations Command in March 2026, in the rank of General.



Katherine Sutton

Assistant Secretary of War for Cyber Policy, U.S. Department of War

Katherine E. Sutton serves as the Assistant Secretary of War for Cyber Policy and the Principal Cyber Advisor to the Secretary of War. In this role, she oversees the Department of War's cyber policies and operations. Prior to her appointment as Assistant Secretary, Ms. Sutton served as the Chief Technology Advisor to the Commander and Director of Pentagon Operations at United States Cyber Command. She advised the Commander on engineering strategies and policies related to workforce management, capability development, acquisition, and budget control. Previously, Ms. Sutton served on the Senate Armed Services Committee as a Professional Staff Member, leading the Subcommittee on Cybersecurity and managing the spectrum, emerging technology, and science and technology portfolios. She also served on the House Armed Services Committee's Emerging Threats and Capabilities Subcommittee. Earlier in her career, Ms. Sutton spent 15 years at Sandia National Laboratories, working on information assurance, cybersecurity, and non-proliferation projects.

SPEAKERS



Christopher Painter

Founding Partner of The Cyber Policy Group and former U.S. Cyber Diplomat

Christopher Painter is a globally recognized leader on cyber policy, cyber diplomacy, cybersecurity and combatting cybercrime. He has been at the vanguard of cyber issues for over 30 years, first as a federal prosecutor handling some of the most high-profile cyber cases in the U.S., then as a senior official at the U.S. Department of Justice, the FBI, the White House National Security Council and, finally, as the world's first cyber diplomat at the U.S. Department of State. Among many other things, Chris is currently a Founding Partner of The Cyber Policy Group.



Pirro Vengu

Minister of Defence, Ministry of Defence of the Republic of Albania

Pirro Vengu was born on April 24, 1986, in Elbasan. Since September 2025, he has been reconfirmed as Minister of Defence, a position he has held since July 2024. Prior to this role, he served as General Executive Director of the Durrës Port Authority (2019–2024). From 2017 to 2019, he was Anti-Corruption Director at the Prime Minister's Office, and from 2013 to 2017, he served as Head of Cabinet at the Ministry of Foreign Affairs. Earlier in his career, Mr. Vengu worked with the European Council on Foreign Relations in Paris as Coordinator of Research Programs (2010–2013) and as Programs Assistant (2009–2010). He completed his secondary education in Humanities in Paris and holds a double Bachelor's degree in History and Philosophy, a Master's degree in Political History, and a second Master's degree in International Relations from institutions in Paris. Mr. Vengu is married and has three children.



Ieva Ilves

Advisor on Cybersecurity and Digital Policy, Ukraine/Latvia

Ieva Ilves brings over two decades of experience in foreign policy, digital transformation, and cybersecurity. She has served as Advisor to the President of Latvia, at Latvia's Ministry of Defence, with the EU Special Representative in Azerbaijan, and at Latvia's Mission to NATO. After Russia's full-scale invasion, she worked with the EU Advisory Mission in Ukraine. Today, she supports Ukraine's Ministry of Digital Transformation, leads a cybersecurity education program in Riga, supports establishment of CISO Campus in Ukraine, and serves on the Board of Latvia's National AI Center. She led Latvia's first national cybersecurity strategy, the establishment of NATO's STRATCOM COE in Riga, and the launch of the "Computer for Every School Child" program. She also co-founded Women4Cyber Latvia and has supported RigaTechGirls and the StartSchool peer-learning platform. Ieva is a graduate of Johns Hopkins University SAIS and is the former First Lady of Estonia.



Radmila Shekerinska

Deputy Secretary General, NATO

Radmila Shekerinska took office as NATO Deputy Secretary General on 2 December 2024. As a former Deputy Prime Minister and Minister of Defence of North Macedonia, Ms Shekerinska has extensive experience as a policy-maker and consensus-builder. She is a champion of gender balance and a steadfast advocate of strong transatlantic relations. Ms Shekerinska served as a member of parliament (2006-2014) and is the only woman to have led any of the major political parties in North Macedonia. As Deputy Prime Minister in charge of European Integration and Foreign Aid Coordination (2002-2006), she oversaw North Macedonia's application to become a candidate country for accession to the European Union. She graduated from the Faculty of Electrical Engineering in Skopje and received her MA in International Relations from the Fletcher School of Law and Diplomacy, Tufts University, USA. She also taught "EU Structures and Institutions" at the University American College of Skopje.

SPEAKERS



Nina Armagno

Lieutenant General, Ret., USSF

Nina M. Armagno served 35 years as a national defense expert and space operations officer in the United States Air Force and the United States Space Force. As the first Lieutenant General confirmed by the Senate into the Space Force, Armagno served as the first director of staff where she orchestrated the establishment of the sixth branch of the U.S. Armed Forces. Commissioned from the U.S. Air Force Academy in 1988, she is the only person to have commanded both launch wings in the Air Force. Today, Armagno serves on the board of directors and strategic advisory groups for several companies, to include Rocket Lab, First Command, Lockheed Martin, United Launch Alliance, and VirnetX. Armagno has received a series of awards, to include the Defense Distinguished Service Medal, the General Jerome F. O'Malley Distinguished Space Leadership Award, the Daughters of the American Revolution Patriot Award, and the Spirit of Space.



Thierry Bauer

Director of Security and Cyber Defence, Eutelsat

Brigadier General (Ret.) Thierry Bauer is a senior French defense and intelligence specialist with over 30 years of experience in air operations, electronic warfare, counter terrorism, and cyber defense. A graduate of the French Air Force Academy, he began his career as an intelligence and electronic warfare officer, taking part in multiple overseas operations in Iraq and the Balkans. His career led him to leadership roles in intelligence collection, including responsibility for operations in Southeast Asia. In 2020, he took command of the Cyber Defense Operations Center, overseeing defensive, influence and offensive cyber operations for the French Armed Forces. Promoted to Brigadier General in 2022, he became Deputy Commander of French Cybercommand. From 2023 to 2025, he served as Technical Director of Military Intelligence, managing expert centers in SIGINT, HUMINT, GEOINT, IMINT, and cyber intelligence, and advancing AI integration in operational systems. He retired in 2025 and joined Eutelsat as Director of Security and Defense Advisor.



Natalie Black

Group Director, Infrastructure & Connectivity, Ofcom

Natalie Black CBE joined Ofcom in 2024 as Group Director for Infrastructure & Connectivity and an Executive Board member, leading Ofcom's work on the implications of Artificial Intelligence. Previously, she was the UK's first His Majesty's Trade Commissioner for Asia Pacific, based in Singapore, where she led trade strategy across 15 countries and served as the UK's first Senior Economic Official to ASEAN. Key achievements included the UK's first Digital Economy Agreement, securing new investment from Australia and Japan, and joining the CPTPP. In the UK, Natalie was Deputy Head of the Prime Minister's Policy Unit, overseeing the 2017 AI Review and establishing the first cross-government Online Harms Unit. She has over 10 years' experience in cyber security, including leading the National Cyber Security Programme. Natalie is a Visiting Professor at LSE, a World Economic Forum Young Global Leader, an LSE and Harvard Kennedy School graduate, and a Fulbright scholar.



Declan Ganley

Chairman/CEO, Rivada Space Networks

Declan Ganley is an entrepreneur and the founder, chairman & CEO of Rivada Networks, a leading innovator in market-driven wholesale wireless network sharing and provider of broadband communications services. Rivada's wholly owned subsidiary, Rivada Space Networks, is currently engaged in a multi-billion-dollar project to deploy the world's first optical, global, LEO "outernet" satellite system. Declan is co-inventor of 48 patents in the wireless sector, including Rivada's core Dynamic Spectrum Arbitrage technology. Rivada's DSA and tiered priority access patents enable the dynamic sharing of wireless networks, lowering barriers to entry and driving innovation in wireless.

SPEAKERS



Thomas Seifert

Chief Financial Officer, Cloudflare

Thomas Seifert is chief financial officer of Cloudflare where he oversees the company's worldwide finance, IT, and data science organizations. Before joining Cloudflare he served as chief financial officer of Symantec. Prior to Symantec he served as chief financial officer at Advanced Micro Devices where he additionally served as interim chief executive officer. Previously, he served in a variety of executive leadership roles before at Infineon and Siemens. He serves on the board of directors of ICEYE, Fruitist, and Personio. Mr. Seifert holds a B.A. in Business Administration and an M.B.A. from Friedrich Alexander University, and an M.A. in Economics from Wayne State University.



Wolfgang Hackenberg

General Management, IABG Defense & Security Services

Wolfgang Hackenberg is an executive at IABG, a Munich-based Defense & Space company serving government, space and defense players with classified security services, spanning satellite tests, war gaming, simulation and testing of defense technologies, and cyber security. - His career includes various executive roles at Airbus, Nokia Networks and IQM, based in Munich, Shanghai, Paris and Helsinki. Wolfgang holds a Physics PhD from the University of Cambridge. - He has been on the Executive Board at Bitkom, Germany's Digital Association, Co-Chair of the Digital Group at BDI, the Federation of German Industries, and founding board member of the Security Network Munich.



Fiona Van Echelpoel

Deputy Director General, DG Market Infrastructure & Payments, European Central Bank

Fiona van Echelpoel is Deputy Director General in the Directorate General Market Infrastructure and Payments of the ECB since January 2018. She has a broad background in central banking, having worked in a number of functions in the market infrastructure and market operations areas of the ECB since its establishment in 1998 and previously for its forerunner the European Monetary Institute; prior to that she worked at the Central Bank of Ireland. She represents the ECB in various European and international fora and chairs the ESCB CCP Working Group, co-chairs the TARGET2-Securities Cooperative Arrangement, the European Forum on the Security of Retail Payments (SecuRePay), and the CPMI IOSCO Implementation Monitoring Sub-Group; she has been chair of the ECB's Internal Crypto Assets Task Force for a number of years and is Rapporteur of the ECB Euro Cyber Resilience Board. She holds a degree in Economics and Politics from University College Dublin.

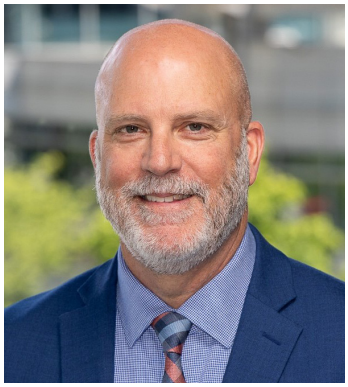


Nathaniel Gleicher

Head of Security Policy and Counter-Fraud, Meta

Nathaniel Gleicher is Meta's global head of security policy and counter-fraud. He is an engineer and a lawyer, and leads strategy at Meta to track and counter determined adversaries that seek to cause serious harms across the internet, including election manipulation, government surveillance, cybercrime, and fraud and scams.

SPEAKERS



Rick Driggers

Global Cybersecurity Lead for Health and Public Service, Accenture

Richard "Rick" Driggers is the Accenture Global Cybersecurity Lead for Health and Public Service, bringing deep expertise in critical infrastructure security, cyber defense operations, and national resilience. As former Deputy Assistant Secretary for Cybersecurity and Assistant Director for Integrated Operations at the Cybersecurity and Infrastructure Security Agency (CISA), he provides strategic leadership across information and operational technology security initiatives. Rick combines more than 15 years of national security experience in the Joint Special Operations Community with over 17 years of homeland security leadership across intelligence, critical infrastructure, and cybersecurity missions. He advises federal clients on threat and vulnerability landscapes, risk management strategies, mission assurance, and resilience of national critical functions. Previously, he served as Principal Deputy Director for Operations at CISA's National Cybersecurity and Communications Integration Center and supported the National Security Council e.g. on data integration. A former U.S. Air Force Combat Controller, he holds numerous special operations qualifications.



Johan Gerber

Executive Vice President, Head of Security Solutions, Mastercard

Johan Gerber is executive vice president and Head of Security Solutions at Mastercard as well as a member of the company's management committee. He is passionate about innovating to secure the digital ecosystem - and enhancing trust across our hyperconnected world. His team works globally to design, develop and scale technology that protects consumers and customers from current and future cyber threats as well as fraud and other financial crimes. During his more than 25 years at Mastercard, Johan has overseen the growth of the company's cybersecurity offering, spearheading the successful acquisition of several security tech companies – including Recorded Future and Minna Technologies – and harnessing Identity, data science and AI to diminish the criminal enterprise. His track record in defining and implementing Mastercard's strategic vision for security has led to accelerated innovation and differentiation, meaning his expertise is widely sought-after across industry. He sits on the Merchant Risk Council advisory board for the Americas. Prior to joining the company, Johan spent 10 years investigating organized crime and financial crime with the South African Police Services. He is a graduate of Rand Afrikaans University, holding a Degree in Forensic Auditing & Accounting.

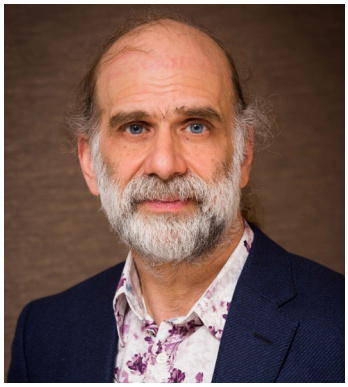


John Miller

General Counsel and Senior Vice President of Policy, Information Technology Industry Council

John Miller is General Counsel and SVP for Policy at the Information Technology Industry Council (ITI), the preeminent global technology trade association. John leads ITI's Trust, Data and Technology team, driving ITI's global policy strategy on cybersecurity, artificial intelligence (AI), supply chain resiliency, privacy, telecommunications, quantum technologies, data governance, and related policy and legal issues. A recognized global expert on technology policy, John has testified before the U.S. Congress on an array of technology policy issues including cybersecurity and privacy and participates in the OECD/GPAI Network of Experts on AI and OECD Expert Community on Data Free Flows with Trust. John has significant leadership experience in U.S. public-private partnerships, including co-chairing the ICT Supply Chain Risk Management Task Force and chairing the IT Sector Coordinating Council. John previously held multiple positions at Intel Corporation including Director of Cybersecurity Policy and is a graduate of Hamilton College and Wisconsin Law School.

SPEAKERS



Bruce Schneier

Lecturer, Harvard University and the University of Toronto

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the Economist. He is the New York Times best-selling author of 14 books – including Rewiring Democracy and A Hacker's Mind -- as well as hundreds of articles, essays, and academic papers. His long-running newsletter and blog, "Schneier on Security," is one of the most popular sources of cybersecurity news on the internet. Schneier is a Fellow and Lecturer in Public Policy at the Harvard Kennedy School and the Munk School at the University of Toronto. He is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University, a board member of the Electronic Frontier Foundation and AccessNow, and an advisory board member of EPIC and VerifiedVoting.org. He is also the Chief of Security Architecture at Inrupt, Inc.



Antti Koskela

President and CEO, WithSecure

Antti Koskela is the President and CEO of WithSecure Oyj, where he leads the company's mission to build a European flagship for cybersecurity and to strengthen Europe's digital sovereignty. He has been a member of the WithSecure Leadership Team since 2021. Before becoming CEO, Antti served as Chief Product Officer, where he shaped the company's SaaS portfolio for the midmarket, with a strong focus on cloud and artificial intelligence. Antti brings deep experience from senior leadership roles across the telecom and software industries. His previous roles include Chief Development Officer at Nokia Software, Chief Technology Officer at Comptel, and several product and business leadership positions at Elisa and Nokia. He is also a board member of QPR Software Oyj. Curious and globally minded, Antti is passionate about advancing cybersecurity transformation in Europe by making modern and scalable security technologies accessible to mid-sized organizations.



Jacob Shapiro

John Foster Dulles Professor in International Affairs, Princeton University

Jake Shapiro is John Foster Dulles Professor in International Affairs and Vice Dean for Strategic Initiatives at the Princeton School of Public and International Affairs. Shapiro co-founded the Empirical Studies of Conflict Project, a multi-university consortium that studies political violence in countries around the world. He leads Princeton's Accelerator Initiative, which is building infrastructure for scientific research on the information environment. Shapiro has published more than 50 articles on conflict, economic development, security, and technology in peer reviewed journals and is author of The Terrorist's Dilemma: Managing Violent Covert Organizations and co-author of Small Wars, Big Data: The Information Revolution in Modern Conflict. Shapiro received the 2016 Karl Deutsch Award from the International Studies Association, given to the scholar within 10 years of earning a Ph.D. who has made the most significant contribution to the study of international relations.



Drew Bagley

Chief Privacy Officer, CrowdStrike

Drew Bagley, Esq. is CrowdStrike's Chief Privacy Officer, leading their privacy and public policy teams and driving global data protection strategy and policy engagement. Since joining CrowdStrike as one of its early employees, he has shaped the company's privacy and public policy strategy throughout its journey from startup through IPO to its position today as a global cybersecurity leader. Mr. Bagley has testified before the U.S. Congress on modernizing federal cybersecurity and regularly engages with government leaders worldwide on issues at the intersection of security, privacy, and emerging technology. He earned his J.D. from UM School of Law, as well as a Master's in Mass Communication Law, a B.S. in Public Relations, and a B.A. in Political Science from the University of Florida. He is a member of the NY State Bar.

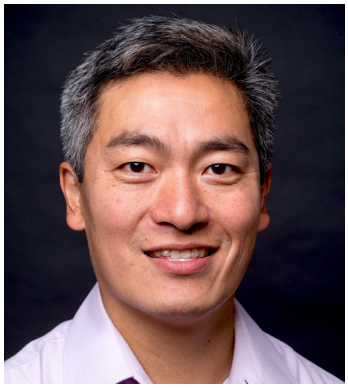
SPEAKERS



Nicole Tisdale

Interim Senior Director to the Cybersecurity Programs, Aspen Digital

Nicole Tisdale is Interim Senior Director and long-time Senior Advisor to the Cybersecurity Programs at Aspen Digital (Aspen Institute). She has eighteen years of experience as a national security attorney at The White House – National Security Council and the U.S. Congress' House Committee on Homeland Security, complemented by consulting for philanthropic and corporate clients. Her expertise spans cybersecurity, counterintelligence, and cyber impacts on rural and low-income communities globally. At the White House, she led cybersecurity advocacy before Congress, driving creation of the $1 billion cybersecurity grant program and passage of the cyber incident reporting law—the most significant cybersecurity law in a decade. She has represented the U.S. in 40 international delegations across 28 countries and spoken at more than 80 conferences in three years. Nicole champions cyber equity through work, including her WIRED article The Hidden Injustice of Cyberattacks. She's a double alumna of The University of Mississippi.



Sounil Yu

Chief AI Officer, Knostic

Sounil Yu is the author and creator of the Cyber Defense Matrix and the DIE Triad. He is currently the cofounder of Knostic, an AI safety startup. Previously, he was the CISO at JupiterOne, CISO-in-Residence at YL Ventures, and Chief Security Scientist at Bank of America. He's a Board Member of the CMMC Cyber Accreditation Body; co-chair of Art into Science: A Conference on Defense; fellow at GMU Scalia Law School's National Security Institute; guest lecturer at Carnegie Mellon; and advisor to many startups.



Igor Andriushchenko

Head of Security, CISO, Lovable

Igor is a founding security engineer, CISO and Head of Security at Lovable. Igor spends his time between guiding AI agents towards fixing security bugs and managing high-level roadmap of Lovable security, compliance and trust. His team ensures that AI-assisted coding is safe and can be relied upon. Previously, Igor worked as a security leader at Sana (acquired by Workday), Shopify, multiple telco and software companies across Europe and North America. He holds MSc. in Machine Learning and Data Mining from Aalto University, and MBA from Blekinge Tekniska Högskola. Igor believes that AGI is already here, and always says "thank you" to his AI agent, to be on the safe side in case of a machine rebellion.



Sergej Epp

CISO & Member of the Executive Team, Sysdig

Sergej Epp secures the infrastructure that cloud and AI runs on. As Global CISO at Sysdig, he leads security, threat research, and IT for the platform protecting workloads across Fortune 500 companies, US and European governments, and leading AI labs — driving adoption of Falco, the open-source runtime security standard embedded across major hyperscalers, 5G networks, and AI infrastructure providers. Previously, as CSO at Palo Alto Networks CEMEA, he advised boards and government bodies including the European Commission and ECB on cyber risk, AI, and emerging technology strategy, and contributed to EU cybersecurity policy as an advisor to ENISA. He has advised management boards of leading European corporates on cybersecurity and AI governance. His research centers on a fundamental asymmetry: AI-powered offense advances faster than defense — and verification cost is the reason why.

SPEAKERS



Jeff Moss

President and Founder of DEF CON

A career spent at the intersection of hacking, cybersecurity and Internet governance gives Mr. Moss a unique perspective as the founder of both DEF CON and Black Hat, two of the world's most influential information security events. Mr. Moss serves on the Board of Directors for Compagnie Financière Richemont SA., and is a member of the UK Government Cyber Advisory Board. Mr. Moss was a member of the CISA Cyber Security Advisory Council where he led the Technical Advisory Council, and was an SGE at the White House ONCD. For 10 years he was a Non-resident Senior Fellow at the Atlantic Council Cyber Statecraft Initiative. He served as the first Chief Security Officer at ICANN, a commissioner on the Global Council on the Stability of Cyberspace (GCSC), and a member of DHS HSAC for 11 years. His most fun work was as a technical advisor for TV series Mr. Robot.



Ariel Herbert-Voss

Co-Founder and CEO of RunSybil

Ariel Herbert-Voss is cofounder and CEO of RunSybil, an automated offensive security company. Previously Ariel was the first research scientist at OpenAI focused on developing algorithmic exploits for large language models and lead the red team engagements for the GPT3 and Codex model releases. Prior to OpenAI Ariel was a Harvard computer science PhD candidate and a Fellow at the Belfer Center for Science and International Affairs.



Daniel Cuthbert

Global Head of Cybersecurity, Santander Group

Daniel Cuthbert is a senior security researcher, technologist, and long-standing contributor to the global cybersecurity community. He serves as Global Head of Cyber Security Research for the Santander Group, where he focuses on advancing detection engineering, cryptographic safety, and applied security research across complex financial systems. Beyond his institutional work, Daniel leads and contributes to a range of open-source and community-led security initiatives, including projects that advance cryptographic transparency, post-quantum readiness, and detection innovation. He sits on the Black Hat Review Board and serves as the Industry Chair of the UK Government's Cyber Security Advisory Board (GCAB), and the UK Department for Science, Innovation, and Technology's Cyber Resilience Expert Advisory Group.



Runa Sandvik

Founder of Granitt

Runa Sandvik is the founder of Granitt, a consultancy focused on security for journalists and other at-risk people around the world. Her work builds upon experience from her time at The New York Times, Freedom of the Press Foundation, and The Tor Project. Runa is a member of the Aspen Institute's Global Cybersecurity Group, an advisor to the Signals Network, and a big fan of indoor skydiving. Originally from Oslo, she's now based in New York.

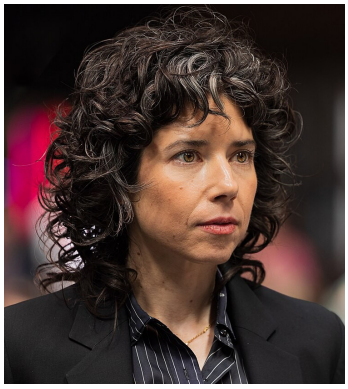
SPEAKERS



Yan Shoshitaishvili

Associate Professor at Arizona State University

Yan Shoshitaishvili is an Associate Professor at Arizona State University, where he pursues parallel passions of cybersecurity research, real-world impact, and education. His research focuses on automated program analysis and vulnerability detection techniques. Underpinning much of his research is angr, the open-source program analysis framework created by Yan and his collaborators. He continues to develop novel approaches to cybersecurity workforce development in his role as Director of the American Cybersecurity Education Institute and has helped advise government policy through CISA's Technical Advisory Council.



Meredith Whittaker

President of the Signal Foundation

Meredith Whittaker is the president of the Signal Foundation and serves on its board of directors. She was formerly the Minderoo Research Professor at New York University (NYU), and chief advisor and former faculty director & co founder of the AI Now Institute. She also served as a senior advisor on AI to Chair Lina Khan at the Federal Trade Commission and was listed among the 100 most influential people in AI by TIME magazine in 2023. Whittaker co-founded M-Lab, a globally distributed network measurement system that provides the world's largest source of open data on Internet performance. She has also worked extensively on issues of data validation, privacy, the social implications of artificial intelligence, the political economy of tech, and labor movements in the context of tech and the tech industry. She has spoken out about the need for privacy and against weakening encryption.



Perri Adams

Former senior official at the Defense Advanced Research Projects Agency (DARPA)

Perri Adams is a former senior official at the Defense Advanced Research Projects Agency (DARPA) where she oversaw research at the intersection of cybersecurity and AI. While there, she created and led several programs, including the AI Cyber Challenge. She serves on a number of conference boards and commissions, and is a frequent speaker. She is currently a fellow at Dartmouth Institute for Security Technology Studies (ISTS) and the founder and CEO of a defense technologies firm.



Jacob Braun

Executive Director of the Cyber Policy Initiative, University of Chicago

Jake Braun is Executive Director of the Cyber Policy Initiative at the University of Chicago Harris School of Public Policy, and CEO of Cambridge Global Advisors. He previously served as the White House acting Principal Deputy National Cyber Director along with several other senior roles in government. Braun is author of Fentanyl: Fighting the Mass Poisoning of America and the Cartel Behind It and Democracy in Danger; How Hackers and Activists Exposed Fatal Flaws in Election Systems, he is co-founder of the Voting Machine Hacking Village at DEF CON and leads production of the Hackers' Almanack

SPACE FOR YOUR NOTES

Confronting the Illusion of Deterrence in the Age of Relentless Cyber Threats



Christopher Painter

Founding Partner of The Cyber Policy Group and former U.S. Cyber Diplomat

For years a debate has raged about deterrence in cyberspace. Is it possible? How does it work? What exactly does deterrence mean? By and large the people involved in these seemingly endless debates have been talking past each other – engaging in discussions akin to how many angels can fit on the head of a pin – because the term "deterrence" carries so much baggage from its use in the nuclear weapons area and seldom do two people mean the same thing when they discuss whether it can be achieved. So let's jettison use of the word and instead focus on what we are trying to achieve. Instead, let's consider what actions can be taken, individually or collectively, to change the adversaries' actions and, relatedly, achieve some level of accountability for malicious actions in cyberspace – and why, so far, we are so bad at taking them.

To level set, I am addressing nation-state, not criminal groups here. Dissuading and sanctioning criminals is pretty well understood – disruption, apprehension and criminal penalties – though, admittedly there are certainly challenges in doing that effectively. And, however you define "deterrence," many think it has worked above the threshold of armed conflict and that at least partially explains why we haven't seen the long feared major infrastructure attack outside an actual military conflict – so the focus should be more on the actions below armed conflict that we see every day. Nor do I consider often promoted "persistent engagement" as a substitute or a silver bullet. Persistent engagement – consistently challenging the adversary and their cyber infrastructure wherever it exists – should be the base, particularly if it's done with partners, but although it makes an adversary's actions more difficult, it doesn't change their overall goals and actions. Similarly, "hardening the targets" and building better resilience is critically important and will make an adversary's actions more difficult, but we have been relatively bad at defence, and it is a companion not a substitute for taking action.

It's also important to set expectations. Unlike the nuclear arena, nothing we do will stop all nation-state malicious activity. As long as the perceived value of an activity outweighs any costs that are imposed, there is no reason to expect that activity to cease. So, for example, it is a fool's errand to expect a halt to traditional espionage. But, unlike nuclear, this isn't binary – there are actions that can be taken that affect adversary conduct.

Yet, there are actions that can be taken. Indeed, there have been a number of initiatives taken in the past, including collective attributions, economic sanctions, use of the European "Diplomatic Toolkit," diplomatic pressure, criminal indictment of nation-state actors, and cyber operations. However, these actions have been somewhat episodic, often late, not calibrated to effect things the adversary prioritizes and lacking high-level political force or certainty. Collective attribution alone helps with accountability but is often ignored or treated as a badge of honor without further concrete action. A good example is the collective attribution of the Russian NotPetya worm announced by the U.S. and others several years ago at the Munich Security Conference – made six months after the event and accompanied by the vague warning that there would be unspecified future consequences. This lack of certainty likely encouraged Russia to engage in further malicious activity as something that was largely costless. If it is going to take many months to announce an attribution have at least one concrete thing you are doing to the adversary to announce at that time.

For those who argue that we cannot affect adversary conduct, I would say that, to date, we haven't really given it a sustained and coordinated try. As noted, there has been a lot of attempts and some good actions, but to be successful those actions need to be certain, coordinated and sustained. There has also been a lot of strategic thinking around this, including a U.S. cyber deterrence strategy created during the first Trump Administration and work on tailoring any responsive actions to particular adversaries and the things they value. The U.S. is now talking about being more "muscular" in cyberspace and the forthcoming U.S. Cyber Strategy reportedly emphasizes cost imposition and more offensive action (though the cyber strategy during the first Trump term made similar statements). Japan and South Korea are implementing "active defence" in cyberspace for the first time. Still all these are additional arrows in the quiver but not the quiver itself. For there to be any real impact on adversary actions or calculus will take more than cyber tools, it will require the coordinated use of all instruments of national power in coordination with partners to bring greater accountability. It's true that the U.S. and others have used a combination of cyber and non-cyber tools in the past but seemingly sporadically and often below the radar. What is usually missing is sustained political will.

To have any long-term impact, cyber-attacks and responses to them need to be treated as a true national security priority not just a rhetorical one – though this has seldom been the case. In the few times this has happened there have been at least some positive results. For example, the only reason China reached a deal with the U.S. on cyber theft of intellectual property – resulting in at least a temporary reduction in this conduct by China – was because President Obama deemed that historically "cyber' issue as one that was so important to national and economic security that was willing to have friction in the overall U.S. China relationship. China agreed to save the larger relationship and because of the threat of sanctions – something that would never have happened if the issue was treated as a cyber issue rather than a political one.

Ransomware became a true national priority meriting President Biden raising it with Putin only after Americans had to wait in line for gas after the Colonial Pipelines and it became a "breadbasket" and thus political issue. Regardless of muscular strategies, capabilities or public statements by cyber focused players, unless the U.S. and other like-minded countries treat this as a real national level political priority, freeing the use of the full panoply of national and collective tools and responses, there is likely to be little real change.

But here is the opportunity. The folks who go to the Munich Cyber Security Conference – both cyber focused and not – mostly accept the relative importance and priority of dissuading and punishing cyber-attacks, but, by and large, those non cyber focused high-level officials at the nearby Munich Security Conference do not. MCSC has been a valuable crucible for discussion on this and other topics and will be again this year, especially as it purposely invites both cyber and non-cyber participants, but it can also serve as a great way to channel these issues across town, especially as many participants in MCSC also attend MSC. The non-cyber focused national security advisors, foreign ministers, legislators, generals and leaders who attend MSC are the ones who need to understand cyber and its long-term consequences, but cyber is often relegated to cyber community cyber side events.

I am not naïve and many difficulties still remain, including the relative lack of leverage with countries like North Korea and Russia, even if these issues are elevated. Consistent collective action among like-minded partners is also a necessity for success – a prospect that may be more difficult in the current frayed geopolitical environment. And there is no guarantee that adversary actions will change if we fall short or making the costs outweigh the benefits. Yet, imposing some costs and sanctioning malicious conduct helps bring some accountability in a time where state sponsored malicious actions that violate International Law and agreed upon norms is on the rise and becoming commonplace. Indeed, International Law and agreed cyber norms of responsible state behavior are little more than words on paper without some effort at enforcement. Nor do I propose that like-minded countries take reckless or unconstrained actions – international law, appropriately calibrated responses and potential escalation (though often overrated) matter. And I am heartened that cyber is much more of a mainstream issue than even ten years ago evidenced in part by militaries increasingly integrating it rather than treating it as a curious separate technical bubble. Still, without this higher-level political recognition, I fear we are doomed to never ending trench warfare, with many not even recognizing the long-term consequences of the fight. So, if you get the opportunity this week, or really any time, break out of the cyber bubble, build on the good discussions you have at MCSC, and try to get those other folks on board. I know many have tried doing this for years, and with all the problems in the world, it may be as hard as achieving so called "deterrence" and accountability in cyberspace, but I think the squeeze is worth the juice.

The official MCSC Jazz Band: FLORIAN BLAU TRIO



Florian Blau (piano), Harry Saltzman (saxophone) and Markus Braun (bass) are skilled professionals on their instruments with a lot of experience and a wide stylistic range always hitting the right notes thanks to their large repertoire. Their performances have enriched Munich Cyber Security Conference for over 10 years now.

Playing Offense: An Aspen Digital Series on Emerging Cybersecurity Trends

Since the rise of cybersecurity, the perceived wisdom for the U.S. government and U.S.-based industry alike has been to prioritize cyber defense. Offensive cyber operations have been perceived as too risky, too escalatory, and too unreliable. The strategic mindset has now shifted - U.S. government and industry leaders are changing course toward not only impeding the effectiveness of attacks but also ratcheting up the consequences to do them in the first place.

Aspen Digital, a program of the Aspen Institute, commissioned members of our U.S. Cybersecurity Group, as well as leaders in government and industry, to establish clear thinking on the future of cyber offensive operations.

- In the inaugural piece, On the Same Page: A Common Language for Understanding Offensive Cyber Action, Paladin Global Institute President Kemba Walden sets the stage for deeper conversations around cyber disruption activities by establishing definitions for what constitutes an offensive cyber act and a guiding taxonomy.
- In Offense Won't Cut it Alone: Don't Forget the Cyber Fundamentals, PwC Head of Global and U.S. Cybersecurity and Privacy Sean M. Joyce identifies three pillars around which to organize an effective cybersecurity strategy rooted in cyber fundamentals: Prevent, Respond, and Recover.
- John Carlin, Strategic Advisor and Chair Emeritus for Cybersecurity, Aspen Digital, answers the question, "What does the law say about hacking back?" in his piece So You Want to Hack Back: Here's What You Should Know. Carlin traces the contours of the law as applied to different types of active defense and offensive cybersecurity measures.
- In Why America Needs a Cyber Force And What It Should Look Like, Mark Montgomery, Senior Director at the Center on Cyber and Technology Innovation, writes that the best and only way to fix cyber readiness challenges is to establish an independent branch of the Armed Forces – a U.S. Cyber Force.
- The most recent piece in the series, Old Tools, New Problems: Why America Doesn't Need Digital Mercenaries, addresses the latest push in Washington, D.C. to retaliate against digital aggression using letters of marque and reprisal. "True deterrence today depends on disciplined public-private coordination, international cooperation, and lawful transparency," writes Devin Lynch, Senior Director at the Paladin Global Institute, "principles far more powerful than any 18th-century license to plunder."

Check out future pieces in this Aspen Digital series at www.aspendigital.org/project/featured-cyber-projects/.

Follow Aspen Digital's programming @AspenDigital on LinkedIn, X, and Bluesky.

Making Resilience Permanent: Bitkom's study on how German companies deal with hybrid threats

Berlin in January of 2026. More than 100,000 people are without electricity for five days in freezing temperatures. Shops have to close, companies cannot continue their business, and more than 2,200 businesses are affected. The reason: an arson attack on a power line. Since this attack, which was claimed by a left-wing extremist group, the threat to critical infrastructure in Germany has finally become the focus of public debate. And this attention is urgently needed. Because the security policy coordinate system has shifted. For years, the spectrum between war and peace has been expanding massively. We are experiencing a strategic grey area in which actors deliberately operate below the classic threshold of war, without being any less destructive. Hybrid is no longer the exception; hybrid is the norm.

Sabotage, cyber attacks, information manipulation and disposable agents are not only aimed at causing damage, but also at creating uncertainty. At casting doubt on the reliability, competence and control of the state. Attacks are taking place in the heart of Europe. Power failures and digital service outages have a direct impact on businesses, public administration and the general population. Russia is already using these tools far into Europe; other state and non-state actors are increasing the vagueness and omnipresence of the threats.

The conclusion must be that resilience cannot be a goal, it must become a permanent state. This applies to the state, but also to society, infrastructure and, in particular, the economy. In the run-up to the Munich Cyber Security Conference, the digital association Bitkom conducted a study for the first time to determine how companies in Germany assess the security situation and how they are preparing for hybrid attacks. According to the study, more than one in five companies (22%) consider a serious crisis as a result of hybrid attacks to be extremely likely, while 61% consider it to be somewhat likely. But what precautions have already been taken in the economy, and what are in the pipeline? How do companies assess the threat to different infrastructures, and how long could they maintain operations in the event of a crisis? How many feel directly threatened by attacks, and from which sources do they expect reliable information? What about the willingness to invest in greater security? And what urgent action must politicians take? The answers to all these questions will be available from 11 February at bitkom.org.

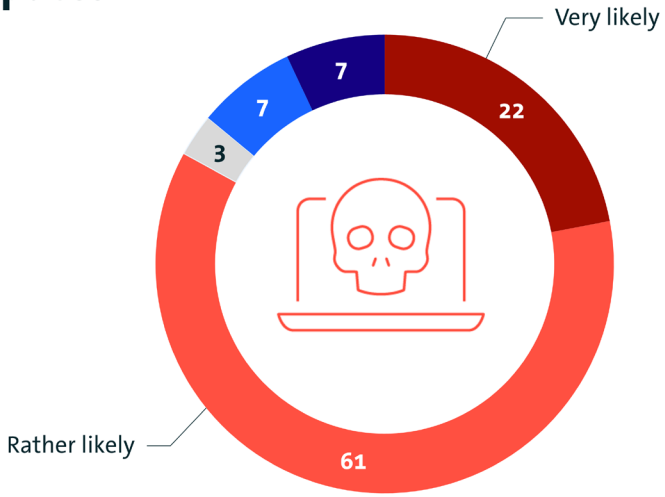
The data and facts should provide the basis for Germany and Europe to work consistently to reduce the existing grey area: through clear red lines and comprehensible consequences. At the same time, through robust resilience that renders malicious activities ineffective. Companies must be prepared for crises, and the study results can help with this. At the same time, it is important to raise public awareness of the importance of resilience against hybrid attacks and of what each and every individual can actively do.

bitkom

German economy anticipates serious hybrid attacks

How likely do you think it is that Germany will experience a serious crisis as a result of hybrid attacks?

- Very unlikely
- Rather unlikely
- Don't know / N. A.



as percentage

Basis: All companies surveyed (I., n=604) | Source: Bitkom Research 2026

bitkom

Geopolitics, AI, and Cyber Risk: Charting a Resilient Security Strategy



Steve Durbin

Chief Executive, Information Security Forum

Steve Durbin is Chief Executive of the Information Security Forum, an independent association dedicated to investigating, clarifying, and resolving key issues in information security and risk management by developing best practice methodologies, processes, and solutions that meet the business needs of its members. ISF membership comprises the Fortune 500 and Forbes 2000.

https://www.linkedin.com/in/stevedurbin/

Cybersecurity is no longer confined to technical domains. It has turned into a strategic area influenced by global instability and the fast changes in artificial intelligence. Organizations that see security as simply a reactive checklist will be vulnerable to attacks from adversaries. These attackers blend geopolitical motives with advanced AI skills to disrupt operations, weaken trust, and gain an advantage. Only by aligning security practice with evolving political, economic, social, technological, legal, and environmental drivers can enterprises maintain agility in the face of mounting threats.

Geopolitics as a Cyber Catalyst

Trade sanctions and tariffs disrupt procurement strategies. They often force organizations to rely heavily on a small number of global suppliers, which increases concentration risk. These dependencies are main targets in proxy conflicts and state-sponsored cyber campaigns. Attackers take advantage of third-party vendors and logistics networks to compromise their intended victims indirectly. At the same time, information-warfare campaigns intensify societal divisions by leveraging social media platforms and deepfake technologies to sway public opinion and steer policy discussions.
To stay ahead, security teams must track regulatory shifts, regional conflicts, and diplomatic flashpoints, linking them to critical assets, supply-chain nodes, and customer-facing channels.

PESTLE: A Structured Lens for Threat Forecasting

To convert broad global developments into specific, actionable threat scenarios, security leaders can turn to frameworks like PESTLE:

Political: State-sponsored cyber activities and changing trade regulations create uncertain and varying risk landscapes. Organizations must quickly respond to changing geopolitical situations.

Economic: Supply chains are increasingly targeted, with attacks often originating from third-party vendors. Financial pressures further increase this exposure.

Social: Social media quickens misinformation and activism. Protests now target corporations in addition to governments, raising reputational and physical security issues.

Technological: AI is transforming both attack and defense. Deepfakes, synthetic personas, and automated tooling are overwhelming old-fashioned controls.

Legal: Sudden regulatory shifts, particularly with respect to trade and data, compel firms to shift operations and compliance tactics.

Environmental: Climate-related disruptions add complexity to logistics and infrastructure resilience.

This targeted approach helps security teams to develop specific incident response plans and bolster their most vulnerable environments.

AI as a Force Multiplier for Cyber Threats

AI is quickly increasing the scale, speed, and complexity of cyber threats. Generative models capable of producing realistic text, audio, and video have lowered the cost of impersonation, making social-engineering attacks more convincing and harder to detect. Deepfakes and synthetic personas can get around technical controls by exploiting human trust. This allows for fraud, extortion, and large-scale influence operations.
Beyond external threats, AI introduces systemic risks to internal defenses: data poisoning can corrupt model behavior, model inversion may expose sensitive training data, and poorly governed training pipelines risk leaking confidential data.
These capabilities aren't limited to nation-states. Criminal groups are increasingly using AI to foment cybercrime. As AI keeps improving, companies must consider it a potential target for attacks. Securing its use requires strong internal controls, careful monitoring and AI security posture management.

Key Pillars of Resilient Operations

To fight these changing threats, organizations must use a method that combines technical skills with smart governance, including:

Continuous scenario planning: Organizations need to go beyond fixed threat reports and start using year-round scenario planning. This means bringing together geopolitical indicators, intelligence feeds, and red-team insights to simulate changing attack paths.

Unified Risk Management and vendor governance: Centralizing supplier assurance and risk tools help remove blind spots in the supply chain. By bringing assessments together on shared platforms, organizations can maintain consistent controls, boost visibility, and include security requirements directly in procurement and vendor contracts.

Securing AI systems: AI threats need both technical defenses and governance oversight. Model-level protections, such as provenance tracking, adversarial testing, and access controls, should work alongside traditional patching and segmentation. Detection systems must be adjusted to spot synthetic content and automated attacks.

Strengthened identity controls: With impersonation risks increasing, organizations need to improve identity verification across all channels. This involves using phishing-resistant MFA, enforcing

least-privilege access, and employing behavioral analytics to spot unusual account activity.

Cross-functional incident response: Effective response to AI-enabled and reputational threats demands coordination across security, legal, communications, and business continuity teams. Updated playbooks should guide rapid, multi-stakeholder action to contain disinformation and operational disruption.

From Foresight to Action

The combination of geopolitical instability and the rapid pace of AI adoption require a change in how we approach cybersecurity. Organizations need to centralize vendor trust, strengthen identity and verification, implement defenses and governance at the model level, and incorporate ongoing scenario exercises into their regular security routines. These actions turn strategic insight into practical resilience.



ACKNOWLEDGMENTS

The MCSC Team would like to thank all speakers, moderators, and contributors who made this conference possible. We are very grateful for the support of the sponsors and security experts for their valuable advice in preparing this event. Our special thanks goes to:

Charlotte Kobel, Despina Spanou, Benedikt Franke, Alexander Kroll, Katherine Getao, Stefani Jones, Kiersten Todt, Sami Khoury, Chris Painter, Jeff Moss, Stormy-Annika Mildner, Annegret Bendiek, Benjamin Bögel, Chiaki Inoue, Molly Hall, Suntka von Halen, Diana Görlich, Janet Bosshammer, David Lashway, Geoff Brown, Christopher Ahlberg, Jonathan Luff, Monica Todros, Preeti Khemani, Antonia Schmidt, Jennifer Kaiser-Steiner, Thilo Kräusslich, Ralf Schneider, Luca Tagliaretti, Andreas Kind, Alexander Schellong, Amely Rechberg, Wolfgang Baare-Schmidt, Damaris Söllner, Zoey Stambolliu, Maria del Pino González, Heinz Stiastny, Nick Brunner, Michael Tagscherer, Nooshin Soltani, Jamie Cox, Richard Vaerst, Kristina Mader, Konstantinos Ntantinos, Ian-tsing Joseph Dieu, Katharina Bertz, Thomas Tarantino, Stefan Lankes, Alexander Wieser, June Chambers, Jens Redmer, Motohiro Tsuchiya, Shinichi Yokohama, Arthur de Liedekerke, Ieva Ilves, Anne Ausfelder, Benno Müchler, Ingrid Dickinson, Jordana Siegel, Timo Blenk, Silke Huber-Voigt, Marina Hoffmann, Marina Geigenberger, Paul Desprez, Philip Stupak, Kerstin Petretto, Sebastian Doedens, Sandra Proske, Amelie Renken, Matthias Bandemer, Ulrike Strauss, Marcel Lewicki, Lukas Baake, Philippa Chancellor-Weale, Susanne Dehmel, Felix Kuhlenkamp, Steven Heckler, Jil Michelle Gonder, Jürgen Kaufmann

MCSC was organized by Security Network Munich and its Partners.

Meet the MCSC Core Team 2026:



Peter Moehring
Director of MCSC
Managing Director of
Security Network Munich



Antje Hickethier
PR and
Event Management



Roberta Walser
Partnerships and
Strategic Development



Kai Hermsen
DECAID Secure



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



Marc Raimondi
Chief of Staff, Silverado
Policy Accelerator



John Mengers
Founder and
Executive Director
of C-Suite Advisors



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

Conference moderators:



Martin Loss
Founder MaLo Blue
Horizons Consulting



Julia Hermann
Head of Digital
Platform Services
at Giesecke+Devrient



Kai Hermsen
DECAID Secure



Bianca Sum Bethune
Head of the Thematic
Platform Cybersecurity
at Bayern Innovativ

Guest Country 2026: Kenya

MCSC welcomes the delegation from Kenya headed by **Dr James Kimuyu**, Director of National Computer and Cybercrime Coordination Committee NC4.

