



SECURITY NETWORK MUNICH
PRESENTS

MCSC

MUNICH CYBER SECURITY
CONFERENCE **2025**

Uncertainty on the Rise: Defining Purpose with Clarity!

Chamber of Commerce Munich (IHK)
13/14 February 2025

Patronized by:

Bavarian Ministry of Economic Affairs,
Regional Development and Energy



Supported by:

AIRBUS

paloalto
NETWORKS

GD Giesecke+Devrient
Creating Confidence

Recorded
Future®

SIEMENS

Google

Meta

aws

TikTok

Allianz

Microsoft

infineon

Lenovo

BRUNSWICK



schwarz digits

W / T H
secure

accenture

GitLab

EY
Building a better
working world

SIDLEY

CLOUDFLARE

Dataminr

Distinguished Guests,

Welcome to Munich, Welcome to the 11th Edition of MCSC.

A long election year lays behind us with the new US Government and the new EU Commission starting their terms while in Germany the upcoming snap election still being only a few days away.

Since our last conference, ongoing geopolitical dynamics - but also technological advances - have presented the world with opportunities, but also pressing challenges demanding the need for urgently adapting our security strategies accordingly; hence the title of this year's edition:

Uncertainty on the Rise: Finding Purpose with Clarity!

"What needs to be done?" is the concurring question throughout all the topics and panels of MCSC 2025. How can we be efficient and purposeful, where do we need to put our focus and concentrate our efforts? "How can we bring our act together?" as one colleague put it in our kick-off meeting in Brussels 4 weeks ago.

We must find formulas and models to combine our efforts across the public and private sectors, across nations and supranational organizations, to become much better in preparing for cyber incidents and in protecting our critical systems and societies as a whole.

It is and must be a joint effort between industry, government, policy makers, regulators, security agencies, but also academia and NGOs; conducted by You, by us, the humans, who are actually in charge.

I wish you all inspiring discussions,

Yours sincerely



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/>.

EDITORIAL



Marco Obiso

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

Editorial Note: Strengthening Global Network Resilience and Cybersecurity

In an increasingly interconnected world, the resilience and high availability of global communication networks are paramount. The International Telecommunication Union (ITU) plays a critical role in ensuring the stability of subsea, space, and critical infrastructure networks, which serve as the backbone of modern digital economies. Through strategic frameworks, collaboration, and innovative solutions, the ITU actively contributes to global connectivity while supporting the United Nations Sustainable Development Goals (SDGs).

Enhancing Subsea and Space Network Resilience

Submarine cables facilitate nearly 99% of international data traffic, making their protection a priority. Recognizing this, the ITU, in partnership with the International Cable Protection Committee (ICPC), established the International Advisory Body for Submarine Cable Resilience. This initiative fosters best practices, international cooperation, and policy development to safeguard these crucial assets (ITU)¹.

Similarly, the ITU's Radiocommunication Sector (ITU-R) ensures efficient, interference-free operation of satellite networks. These regulations are fundamental to sectors such as disaster management, navigation, and global broadcasting, reinforcing the availability of space-based communications.

Driving Connectivity Through the Connectivity Planning Platform (CPP)

Currently in development, the Connectivity Planning Platform (CPP) is an open-source, AI-powered, data-driven initiative designed to optimize broadband infrastructure deployment, particularly in underserved regions. By integrating diverse datasets and utilizing artificial intelligence for predictive analytics and dynamic modeling, CPP will enable governments and regulators to make more accurate, evidence-based decisions. This innovative approach aims to enhance network resilience and ensure sustainable, data-informed connectivity solutions.

Cybersecurity as a Cornerstone of Digital Trust

Beyond infrastructure, cybersecurity is a growing concern. The ITU's Global Cybersecurity Agenda (GCA) fosters international collaboration to strengthen digital security frameworks. Additionally, the Global Cybersecurity Index (GCI) evaluates national cybersecurity preparedness, encouraging stronger defenses and cooperation among nations (ITU)².

Contributions to UN Sustainable Development Goals (SDGs)

These initiatives directly align with SDG 9 (Industry, Innovation, and Infrastructure) and SDG 17 (Partnerships for the Goals). By fortifying network resilience and cybersecurity, the ITU is fostering sustainable industrialization, innovation, and robust international collaboration.

The ITU's proactive efforts in ensuring the resilience of subsea, space, and critical networks coupled with a strong cybersecurity framework are essential for a digitally secure and connected future. As technology continues to evolve, the ITU remains at the forefront, shaping a resilient and sustainable global digital ecosystem.

References

1. ITU. "International Advisory Body for Submarine Cable Resilience." Retrieved from <https://www.itu.int/en/mediacentre/Pages/PR-2024-11-29-advisory-body-submarine-cable-resilience.aspx>
2. ITU. "Global Cybersecurity Agenda." Retrieved from <https://www.itu.int/en/action/cybersecurity/Pages/default.aspx>

IMPRINT

Publisher:
Security Network Munich

Layout:
Zeilbeck Design Company

© Security Network Munich, 2025
All rights reserved

Uncertainty on the Rise: Defining Purpose with Clarity!

THURSDAY, FEBRUARY 13TH

1:30–1:35 p.m.	Welcome	Claudia Eckert Chairwoman Security Network Munich
1:35–2:20 p.m.	Opening Panel: Uncertainty on the Rise: Where to put the Focus in Cybersecurity in 2025? Moderator: Siobhan Gorman Partner and Cybersecurity, Data & Privacy Global Lead at Brunswick Group	Felix Barrio Director General of INCIBE Keiichi Ichikawa Assistant Chief Cabinet Secretary & Deputy National Security Advisor at the Cabinet Secretariat of Japan Sami Khoury Government of Canada Senior Official for Cyber Security Marko Mihkelson Member of the Estonian Parliament, Chairman of the Foreign Affairs Committee Annegret Bendiek Senior Fellow at SWP, Germany
2:20–3:00 p.m.	Engaging the Private Sector or How can PPPs be successful? Moderator: Geoff Brown President and Chief Operating Officer at Arete	Miguel De Bruycker Managing Director General of the Centre for Cybersecurity Belgium Jim Higgins CISO at Snapchat Thomas Seifert CFO at Cloudflare Max Peterson Vice President of Sovereign Cloud Amazon Web Services
3:00–3:45 p.m.	Spotlight: New Frontiers in Cyber Security Moderator: Ciaran Martin Professor at the Blavatnik School of Government, University of Oxford	Noboru Nakatani Corporate Executive Vice President and CSO at NEC, Japan Marco Obiso Chief of Digital Networks and Environment Department, Telecommunication Development Bureau, ITU. Wendi Whitmore SVP of Unit 42 at Palo Alto Networks Oleksandr Potii Chairman of SSSCIP of Ukraine Nathaniel Gleicher Global Head of Counter-Fraud and Security Policy, Meta
3:45–4:15 p.m.	Coffee Break	
4:15–4:50 p.m.	Fireside Chat: Intelligence View Moderator: Christopher Ahlberg Co-Founder and CEO at Recorded Future	Carl Bildt Former Prime Minister of Sweden Sir Jeremy Fleming Former Head of UK Intelligence, Cyber and Security Agency, GCHQ Dag Baehr Vice President, Federal Intelligence Service (BND)
4:50–5:35 p.m.	Second Panel: Human League: Leadership and Engagement for Managing Future Cyber Risks Moderator: Kiersten Todt Former Chief of Staff at CISA and President of Wondros	Paul M. Nakasone Former NSA Director and Founding Director of the Vanderbilt University Institute of National Security Peter Kant Chairman and CEO at Enabled Intelligence Ann Cleaveland Executive Director of the UC Berkeley Center for Long-Term Cybersecurity Johan Gerber Executive Vice President and Head of Security Solutions at Mastercard Natalia Oropeza Global Chief Cybersecurity Officer at Siemens

5:35–5:40 p.m.	Setting the Scene	Catherine De Bolle Executive Director of Europol
5:40–6:30 p.m.	Heavy Infiltrations: Typhoon Talk – Law Enforcement Reloaded Moderator: David Lashway Partner Sidley Austin LLP	Lisa Monaco Former U.S. Deputy Attorney General Carsten Meywirth Head of the Cybercrime Unit, Federal Criminal Police Office (BKA) Sandra Joyce Vice President Google Threat Intelligence Group Edvardas Šileris Head of Cybercrime Centre Europol, Netherlands Dmitri Alperovitch Co-Founder and Executive Chairman of Silverado Policy Accelerator
6:30–6:55 p.m.	Coffee Break	
6:55–7:20 p.m.	Trans-Atlantic View Moderator: David Sanger White House and National Security Correspondent, The New York Times	Anne Neuberger Former Deputy National Security Advisor for Cyber and Emerging Technologies at The White House Sir Julian King Former EU Commissioner
7:20–7:55 p.m.	Spotlight: Risky Concentrations: Resilience on the Edge Moderator: Sasha O’Connell Senior Director for Cybersecurity Programs at The Aspen Institute	Claudia Plattner President of the German Federal Office for Information Security (BSI) Drew Bagley Vice President and Counsel for Privacy and Cyber Policy at CrowdStrike Pascal Andrei Senior-Vice President Chief Security Officer at Airbus
7:55–8:00 p.m.	Greeting by State Secretary	Tobias Gotthardt Bavarian Ministry of Economic Affairs
8:00 p.m.	Dinner Reception	

NEW: PARALELL BREAK-OUT SESSIONS

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

2:30–3:15 p.m.	Break-out session on Ukraine: Cyber Resilience During the War Moderator: Ieva Ilvesa Advisor to Ministry of Digital Transformation of Ukraine/ WithSecure, Finland	Natalia Tkachuk Head of Cyber and Information Security Directorate, National Security and Defence Council of Ukraine Yegor Aushev CEO of Cyber Unit Technologies & Director of Kyiv International Cyber Resilience Conference, Ukraine Ihor Malchenyuk Director of Cyber Defence Department, State Service of Special Communications and Information Protection of Ukraine
----------------	--	--

FRIDAY, FEBRUARY 14TH

8:30–9:15 a.m.

Technology Matters:
AI, Quantum Computing,
promising perspectives?

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

Gerhard Fettweis

Vodafone Chair Professor at Technical University Dresden

Michele Mosca

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

Jacky Fox

Global Cyber Security Strategy Practice Lead, Accenture

Thomas Saueressig

Board Member of SAP

Eva Maydell

Member of the European Parliament

9:15–9:30 a.m.

Focus India

Cyber Resilience Agenda 2025

Moderator: Ralf Wintergerst

President of Bitkom,
Group CEO of Giesecke+Devrient

Nandan Nilekani

Co-Founder and Chairman of Infosys Limited, India

9:30–10:15 a.m.

Cyber Defense in 2025

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

LtGen Michael Vetter

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

Hannah Neumann

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

Carl-Oskar Bohlin

Swedish Minister for Civil Defence

MajGen Zac Stenning

Director of Strategy and
Assistant Chief at UK Strategic Command

Chris Inglis

Former National Cyber Director at The White House, USA

10:15–10:45 a.m.

**Preparedness and Resilience
in 2025: What to Take Out From the
Niinistö Security Report?**

Moderator: Oliver Rolofs

Co-Founder of MCSC & Founder and
Managing Partner of Commvisory

Despina Spanou

Principal Adviser in the European Commission
for Cybersecurity Coordination

Rolf Schumann

Co-CEO of Schwarz Digits, Germany

Volodymyr Lutchenko

CTO of Ukraine's largest mobile operator

10:45–11:15 a.m.

Coffee Break

11:15–11:25 a.m.

Vantage Point

Audrey Tang

Cyber Ambassador, former Minister of Digital Affairs, Taiwan

11:25–11:35 a.m.

Three Questions for

Moderator: Stormy-Annika Mildner
Executive Director Aspen Institute
Germany

Hanno Pevkur

Minister of Defence of the Republic of Estonia

11:35–12:20 a.m.

**Information Ecosystems in a
Changing World**

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

Lisa Kaplan

Founder & CEO, Alethea

Ginny Badanes

General Manager of Democracy Forward at Microsoft

Maia Mazurkiewicz

CEO of PZU Foundation & Co-Founder of Alliance4Europe

Nicola Hudson

Partner and Cybersecurity, Data & Privacy Global Lead at
Brunswick Group

Vilas S. Dhar

President at Patrick J. McGovern Foundation

12:20–12:35 p.m.

Keynote

Henna Virkkunen

Executive Vice-President of the European Commission

12:35–1:20 p.m.

Security Sovereignty by Regulation?

Moderator: Alexander Evans
Associate Dean, London School of Economics

Dennis-Kenji Kipker

Research Director at Cyber Intelligence Institute

Axel Deininger

President of ECSO & CEO of securnet

Hans de Vries

Chief Cybersecurity and Operations Officer at ENISA

Thomas Rosteck

Division President for CSS at Infineon Technologies

Jason Ruger

CISO at Lenovo

1:20–1:55 p.m.

Lunch Break

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



1:55–2:00 p.m.

Opening Remarks

Jeff Moss

President and Founder of DEF CON

2:00–2:40 p.m.

First Panel:

AI, Automated Attack & Defense

Moderator: Jeff Moss

President and Founder of DEF CON

Perri Adams

Special Assistant to the Director of DARPA

David Weston

Vice President, Enterprise and OS Security at Microsoft

Yan Shoshitaishvili

Assistant Professor at Arizona State University

2:40–3:20 p.m.

Second Panel:

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

Moderator: Jeff Moss

President and Founder of DEF CON

Bill Woodcock

Secretary General of Packet Clearing House

Linus Neumann

Chaos Computer Club

Joel Krooswyk

Federal CTO at GitLab

3:20–4:00 p.m.

Closing Panel:

All Hands on Deck, Capacity Building,
The Next Generation

Moderator: Philip Stupak

Former Assistant National Cyber
Director at The White House

Jake Braun

Executive Director of the Cyber Policy Initiative,
University of Chicago

Christopher Painter

Former President of the Global Forum on
Cyber Expertise Foundation

Carole House

Former Special Advisor for Cybersecurity at NSC, USA

4:00 p.m.

End

NEW: PARALELL BREAK-OUT SESSIONS

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

10:00–10:45 a.m.

Charter of Trust:

Introductory Remarks by **Sumit Chanda**,
Group CISO, Eviden followed by panel

Moderator: Ralf Schneider

Senior Fellow and Head of Cybersecurity
and NextGenIT Think Tank, Allianz

Mikko Hyppönen

Chief Research Officer, WithSecure

Lars König

Technical SOC Lead, Allianz

Natalia Oropeza

Global Chief Cybersecurity Officer at Siemens

Sudhir Ethiraj

Global Head of Cybersecurity Office & CEO
Business Unit Cybersecurity Services, TÜV SÜD

11:00–12:00 a.m.

Meta: Understanding the Impact of Fraud and Scams through a National Security Lens

By invitation only. Please contact ingriddickinson@meta.com for more info

DISTINGUISHED GUEST OF HONOR



Carl Bildt

Former Prime Minister of Sweden

Carl Bildt served as both prime minister and foreign minister of Sweden. Under his leadership, the government initiated major liberal economic reforms and negotiated Sweden's accession to the EU. Previously, he served as EU special envoy to the former Yugoslavia, high representative for Bosnia and Herzegovina, UN special envoy to the Balkans, and co-chair of the Dayton Peace Conference. He also chaired the Global Commission on Internet Governance. In 2021, he was appointed WHO special envoy for the Access to COVID-19 Tools Accelerator.

CONFERENCE MODERATORS:



Julia Hermann

Chief Information Security Officer at infodas,
an Airbus Cyber & IT subsidiary

Julia Hermann is Chief Information Security Officer at infodas, an Airbus Cyber & IT subsidiary. She is a recognized leader in the cybersecurity field with more than 20 years of experience across various industries. Her expertise spans security strategy and management, security architecture, cyber defense, and the establishment, management, and development of international teams. Passionate about advancing cybersecurity and empowering others, she acts as a role model, keynote speaker and panelist, and mentor. She also serves as a trusted advisor and subject matter expert to several strategic working groups within ISACA Global, and advocates for diversity and inclusion in the security and tech industry. As Vice President of the ISACA Germany Chapter, she spearheads the She@ISACA initiative, dedicated to empowering and advancing women in cybersecurity.



Kai Hermsen

twinds Foundation

Kai Hermsen is a "trust in tech" activist dedicated to helping people understand digital technologies and their societal impacts. As co-founder of the "twinds foundation", he focuses on developing open-source disposable identities to build digital trust. He strategically advises organizations on digital trust and cybersecurity, including the "Security Network Munich" where he serves as a strategic advisor and moderates community events. At Siemens, he led the "Charter of Trust", a global initiative of 17 corporations working to enhance digital security. Through his work with "Identity Valley" and its partners, he actively promoted responsible digital practices. As a father of two, he is committed to finding a balanced approach that enables both professional excellence and a fulfilling family life.

SPEAKERS



Henna Virkkunen

Executive Vice-President of the 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).



Siobhan Gorman

Partner and Cybersecurity,
Data & Privacy Global Lead at Brunswick Group

Siobhan Gorman is a Partner in the Washington, D.C. office of the Brunswick Group, where she concentrates on crisis, cybersecurity, public affairs, and media relations. Siobhan has also led a range of cybersecurity, public affairs, litigation, and corporate reputation projects in the financial, retail, airline, and technology sectors. Prior to joining Brunswick, Siobhan had a successful 17-year career as a reporter, most recently at The Wall Street Journal. At The Journal, she covered a range of national security and law enforcement topics, including counterterrorism, intelligence, and cybersecurity. She began her career as a researcher for a columnist at The Washington Post. She has been nominated three times for the Pulitzer Prize and is a graduate of Dartmouth College.



Felix Barrio

Director General of INCIBE

Félix Antonio Barrio Juárez holds a Masters in Software and Systems Engineering and a University Expert Diploma in Management and Administration of Information and Technologies from the University of Alcalá and a Doctorate in Science and Technology Management from the University of Salamanca. He has held various positions at the Universities of Burgos, León and Salamanca. Between 2007 and 2014 he was Manager at the National Institute of Communication Technologies and between 2014 and 2019 at the Spanish National Cybersecurity Institute (INCIBE). Between 2019 and 2020 he was director of the Cybersecurity Hub at Tec de Monterrey. Later he was appointed Deputy Director of Cybersecurity for Society and Business and is currently General Director of INCIBE. He has delivered various postgraduate seminars at different universities and teaches on several Masters programmes in IT Governance and Information Security Management Systems.

SPEAKERS



Keiichi Ichikawa

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

Mr. Ichikawa is the Assistant Chief Cabinet Secretary and Deputy National Security Adviser in the Cabinet Secretariat. Previously, he served at the Ministry of Foreign Affairs for over thirty years mainly in foreign policy coordination. Most recently, he served as the Deputy Minister for Foreign Policy, taking charge of the foreign policy planning and its coordination. He also served as the Executive Assistant to the Chief Cabinet Secretary. Mr. Ichikawa is a graduate of University of Tokyo, where he earned a Bachelor of Laws. He also received an Executive Master's in International Relations from Syracuse University's Maxwell School of Citizenship and Public Affairs.



Sami Khoury

Government of Canada Senior Official for Cyber Security

Sami Khoury serves as the Government of Canada Senior Official for Cyber Security, providing cyber security expert advice and guidance to deputy ministers and senior officials across the Government of Canada. This role, with Sami's extensive experience and knowledge, is critical to safeguarding Canada's digital infrastructure and advancing our national security interests. Previous to this, Sami was the Head of the Canadian Centre for Cyber Security from 2021 to 2024. Over the years, he has held various operational and leadership roles. He served as Assistant Deputy Minister for Enterprise Technologies and Solutions. In this capacity, he was CSE's CIO and led CSE's Research program and the 24/7 Operations Centre. Sami holds a Bachelor's degree in Computer Engineering and a Master of Applied Science from Concordia University in Montreal. Sami's contributions have been recognized through various accolades, including the Queen Elizabeth Diamond Jubilee Medal and the APEX Award of Excellence for Innovation.



Marko Mihkelson

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

Marko Mihkelson is an Estonian politician and currently serves as the Chairman of the Foreign Affairs Committee in the Estonian Parliament (Riigikogu). Representing the Reform Party, which aligns with the Renew Europe group, Mihkelson has been a key figure in Estonian politics since his first election in 2003. Throughout his career, he has held various leadership roles, including Chair of the EU Affairs and National Defense Committees. Before entering politics, Mihkelson made significant contributions in media and Russian studies. He served as Editor-in-Chief of Postimees, Estonia's largest daily newspaper, from 1997 to 2000, and earlier as the paper's Moscow correspondent. From 2000 to 2003, he directed the Baltic Centre for Russian Studies. Holding a Master's degree in History from the University of Tartu, Mihkelson is the author of notable books on Russian geopolitics, such as *Russia: In Dusk and Dawn* (2010) and *The Disruptive Era* (2018). In addition to his parliamentary role, Mihkelson chairs the Council of Foreign Relations of Estonia and is a member of the European Council of Foreign Relations and the International Centre for Defence and Security (ICDS), contributing to Estonia's global diplomatic strategy and defense initiatives.

SPEAKERS



Annegret Bendiek

Senior Fellow at SWP, Germany

Dr. Annegret Bendiek is Co-Lead of the Cluster “Cybersecurity and Digital Policy” and Senior Fellow in the EU/Europe Research Division at the German Institute for International and Security Affairs (SWP Berlin). She has researched European Foreign and Security Policy since 2005, with a special focus on the challenges of digitalisation and new emerging threats for foreign and security policy. In 2014, Annegret served in the Policy Planning Unit of the German Federal Foreign Office to work for the „Review 2014: Fresh look on Foreign Policy of the Federal Republic of Germany“ initiated by the former Foreign Minister Steinmeier. In 2013, she was Robert Bosch Fellow at the Transatlantic Academy „The Future of the Liberal Order“ and Visiting Fellow at German Marshall Fund in Washington, D.C. She spent the 2021/22 fall term as a Visiting Professor at the Centre for European Studies at Carleton University, Canada. From October 2022 until September 2023, she held the Chair of European Studies at the University of Osnabrück. She has repeatedly testified before the Committee for European Affairs of the German parliament and advises governmental and EU institutions in different aspects of the Common Foreign and Security Policy. She has earned her habilitation degree from the University of Osnabrück in 2023.



Geoff Brown

President and Chief Operating Officer at Arete

Geoff Brown is President and COO at Arete, leading strategic growth in the risk, cybersecurity, technology, services, and government sectors. Previously, Geoff was with Recorded Future, where he led the delivery of the company’s premier intelligence cloud offering to global governments. From 2016 to 2022, he served as Chief Information Security Officer for the City of New York, founding and leading NYC Cyber Command in 2017. This agency consolidated the city’s cybersecurity strategy, set citywide policies, directed incident responses, optimized cybersecurity spending, and advised City Hall and agencies. Geoff also launched NYC Secure, a public-facing cybersecurity initiative for New Yorkers. Geoff has a background in financial services and with the U.S. Federal Government, including the 9/11 Commission. He is a visiting professor at the Middlebury Institute of International Studies and an advisor for NYU’s Cybersecurity and Risk Strategy program.



Miguel De Bruycker

Managing Director General of the Centre for Cybersecurity Belgium

After completing his studies at the Royal Military Academy in Brussels, Miguel De Bruycker served as a company commander in Germany for two years. He then transitioned to the information technology branch within the Belgian Defence, where he was responsible for implementing Local Area Networks and services across more than 20 sites in Belgium. He later joined the Military Staff and completed his master’s degree in Information Technologies at the Vrije Universiteit Brussel. In 2005, he contributed to a long-term vision document and wrote a dissertation on Cyber Defence. He joined the General Intelligence and Security Service, where he was responsible for securing classified networks and creating the first cyberdefence unit in Belgium. Since 2008, he and his cyber team have been involved in handling all major cyber incidents in Belgium. In 2012, he took the initiative to write the first National Cybersecurity Strategy. On August 17, 2015, he founded the Centre for Cybersecurity Belgium, where he continues to serve as Director General. Under his visionary leadership, this national centre has significantly enhanced Belgium’s cybersecurity, making it one of the least cyber-vulnerable countries in the EU.

SPEAKERS



Jim Higgins

CISO at Snapchat

Jim Higgins, CISO of Snap Inc., is a seasoned technology and business leader with over 30 years of experience in the high-technology sector, specializing in Information Security and public-private collaboration. Jim has held senior leadership roles at some of the world's most influential companies, including serving as Director of Product Security at Google, and as CISO at Block, Inc. (formerly Square, Inc.), and other fortune 100 entities. His expertise spans product, offensive, and cloud security, with a deep focus on emerging cyber threats and their impact on both private enterprises and public institutions. He serves as a senior cybersecurity advisor at American University and has been a member of the National Security Agency Advisory Board (NSAAB) since 2023. He was also instrumental in helping the Linux Foundation establish the Open Source Security Foundation. As CISO of Snap, Jim continues to leverage his expertise and leadership to protect users and innovate in a rapidly evolving security landscape.



Thomas Seifert

CFO at Cloudflare

Mr. Seifert has served as our Chief Financial Officer since June 2017. Prior to joining Cloudflare, he served as Executive Vice President and Chief Financial Officer of Symantec Corporation, a provider of cybersecurity software and services, from March 2014 to November 2016 and served in an advisory capacity to Symantec from December 2016 to March 2017. From December 2012 to March 2014, Mr. Seifert served as Executive Vice President and Chief Financial Officer of Brightstar Corp., a wireless distribution and services company. From October 2009 to September 2012, he served as Senior Vice President and Chief Financial Officer at Advanced Micro Devices., a semiconductor company where he additionally served as Interim Chief Executive Officer from January 2011 to August 2011. Mr. Seifert currently serves as a member of the board of directors of First Derivatives plc, an ultra-high-performance analytics software company. He previously served on the board of directors of CompuGroup Medical SE, an eHealth provider, and IPG Photonics Corporation, a manufacturer of fiber lasers. Mr. Seifert holds a B.A. in Business Administration and an M.B.A. from Friedrich Alexander University, and an M.A. in Mathematics and Economics from Wayne State University.



Max Peterson

Vice President of Sovereign Cloud Amazon Web Services (AWS)

Max Peterson is the vice president (VP) of Amazon Web Services (AWS) Sovereign Cloud. He leads efforts to ensure all AWS customers around the world have the most advanced set of sovereignty controls, privacy safeguards, and security features available in the cloud. Prior to his current role, Peterson served as the VP of AWS Worldwide Public Sector (WWPS) and created and led the WWPS International Sales division with a focus on empowering government, education, healthcare, aerospace and satellite, and nonprofit organizations to drive rapid innovation while meeting evolving compliance, security, and policy requirements. Peterson has over 30 years of public sector experience and served in other leadership technology roles before joining Amazon. Peterson has earned both a Bachelor of Arts in Finance and Master of Business Administration in Management Information Systems from the University of Maryland.

SPEAKERS



Ciaran Martin

Professor at the Blavatnik School of Government,
University of Oxford

Professor Ciaran Martin, CB, is a Professor of Practice at the Blavatnik School of Government at the University of Oxford, as well as a managing director at Paladin Capital and the holder of several other advisory roles in private sector cyber security. He writes and speaks frequently on cyber security in major outlets across the world and was named one of the most influential people in European technology by Politico in 2022. From 2014 until 2020 he set up and then led the United Kingdom's world-leading National Cyber Security Centre, within the intelligence agency GCHQ on whose board he sat. This was the culmination of a 23-year career in UK public service which saw him serve in senior roles in national security, constitutional and economic policy.



Noboru Nakatani

Corporate Executive Vice President and CSO at NEC, Japan

Mr. Nakatani is in charge of the NEC's group cyber security strategy and business as Corporate EVP and Chief Security Officer, NEC Corporation, and President and CEO, NEC Security, Ltd., Tokyo, Japan(2024-). Mr. Nakatani served as the Executive Director of INTERPOL Global Complex for Innovation (2012-2018) to enable law enforcement to better combat cybercrime after the Director of Information Systems and Technology (2008-2011) and the Assistant Director of INTERPOL's Financial and High Tech Crime (2007-2008) at INTERPOL's General Secretariat in Lyon, France. He joined the National Police Agency (NPA) of Japan in 1993 and has held various posts such as the Senior Assistant Director for Cyber Crime Division and the Director of Transnational Organized Crime Office. He joined Yahoo Japan as Executive Vice President (2019-2022) after serving 26 years in the NPA.



Marco Obiso

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

Mr. Marco Obiso is Chief of the Digital Network Society Department in the Telecommunication Development Bureau of the International Telecommunication Union (ITU), the lead UN-specialized agency for ICTs, and has been working in the field of Information and Communication Technologies for the past two decades. He has been operating in several ICT related domains such network infrastructure and digital services development, IT Service Management, Internet governance and information security. He facilitates the work of ITU in elaborating digital strategies, promoting digital transformation, providing technical assistance at the national level and strengthening coordination and cooperation within the UN system.

SPEAKERS



Wendi Whitmore

SVP of Unit 42 at Palo Alto Networks

Wendi Whitmore serves as senior vice president for Unit 42 at Palo Alto Networks. She is a globally recognized cybersecurity leader, with two decades of experience building incident response and threat intelligence teams that have helped solve some of the world's largest breaches. Wendi leads Unit 42, a team of elite incident responders, security consultants and world-renowned threat researchers. The team helps organizations tackle the most complex cyberthreats - from ransomware to state-sponsored espionage. She is the chair of the industry advisory board for the Duke University Master of Engineering in Cybersecurity (MECS) and a member of the World Economic Forum's Global Future Council on Cybersecurity. Wendi was previously an inaugural member of the Cyber Safety Review Board launched by the United States Department of Homeland Security. She began her career as a Special Agent with the Air Force Office of Special Investigations. She previously held executive level positions at IBM, CrowdStrike and Mandiant.



Oleksandr Potii

Chairman of SSSCIP of Ukraine

Oleksandr Potii earned his PhD in communication security from Kharkiv Military University and became DScTech at Kharkiv National University of Air Force. His areas of research include information protection standards, cybersecurity and cryptography. He has more than 25 years of experience in military service, and 20 years of academic and pedagogical experience. Before joining the State Service, he has held different technical and administrative positions at important educational institutions, such as Kharkiv National University of Radio Electronics and National Aerospace University "Kharkiv Aviation Institute". At his current position, Brigadier General Potii is responsible for a range of important areas, including among others the development and implementation of policies regarding cybersecurity and technical information protection in Ukraine. Oleksandr Potii is a laureate of the National Prize of Ukraine named after Borys Paton (2021). He authored 5 manuals, more than 100 research articles, and developed several specialised university courses in areas of his expertise.



Nathaniel Gleicher

Global Head of Counter-Fraud and Security Policy, Meta

Mr. Nathaniel Gleicher is the Head of Security Policy at Meta, where he leads the company-wide effort to counter emerging and persistent threats across our platforms, including influence operations, cyber-espionage, and cybersecurity risks. He is an engineer and lawyer, and has worked in security for more than fifteen years. He has taught computer science, built and secured computer networks, and prosecuted cyber crime at the U.S. Department of Justice, served as director for cybersecurity policy at the National Security Council (NSC) in the White House, and as head of cybersecurity strategy at Illumio. At the NSC he developed U.S. government policy on key technology and cybersecurity challenges, including encryption, cyber deterrence, internet governance, and network security.

SPEAKERS



Christopher Ahlberg

Co-Founder and CEO at Recorded Future

Dr. Christopher Ahlberg is the co-founder and CEO of Recorded Future, the world's largest threat intelligence company, acquired by Mastercard in 2024. Since co-founding the company in 2009, he has played a key role in shaping its growth as a global leader in intelligence-driven security. Previously, he co-founded Spotfire, later acquired by TIBCO. He also serves as Chairman of Hult International Business School.



Sir Jeremy Fleming

Former Head of UK Intelligence, Cyber and Security Agency, GCHQ

Sir Jeremy Fleming KCMG CB served as the 16th Director of GCHQ. GCHQ has a uniquely broad mission covering global intelligence, cyber security and cyber operations. Prior to this appointment, Jeremy spent 25 years in MI5, finishing as Deputy Director General with responsibility for investigations and operations. He has gained a reputation as an influential public voice on national security, cyber and technology and now advises global businesses on these themes.



Dag Baehr

Vice President, Federal Intelligence Service (BND)

Major General Dag Baehr has been Vice President and Senior Officer at the Federal Intelligence Service since 2023. He has been in the Bundeswehr since 1985 and has held a wide range of positions, including in the Federal Ministry of Defense, at NATO, as commander of the Special Forces Command from 2013-17, and most recently as Deputy Commander of the Strategic Reconnaissance and Commander of the Sensors and Effects Command. Baehr has been deployed overseas numerous times, including as Commander of a Special Operations Task Force as well as multiple deployments to war zones and crisis areas on secondment to other departments and federal authorities.



Paul M. Nakasone

Former NSA Director and Founding Director of the Vanderbilt University Institute of National Security

A native of White Bear Lake, Minnesota, Paul M. Nakasone is the Founding Director of Vanderbilt University's Institute of National Security, focused on building the next generation of leaders with the knowledge, skills, and abilities to succeed in a dynamic security environment. Paul served for more than three decades in the United States Army, including nearly six years as the commander of US Cyber Command and the director of the National Security Agency.

SPEAKERS



Kiersten E. Todt

Former Chief of Staff at CISA and President of Wondros

Kiersten Todt is the President of Wondros, a service-driven creative company that specializes in brand storytelling, strategic communications, and building transformative campaigns. She is the former Chief of Staff of the Cybersecurity and Infrastructure Security Agency (CISA), where she was responsible for agency priority planning, strategy, and allocation of resources. She also served as Executive Director of President Obama's Commission on Enhancing National Cybersecurity and as a professional staff member in the U.S. Senate, where she co-drafted legislation to create the Department of Homeland Security. Ms. Todt co-founded, with leading industry CEOs, the Cyber Readiness Institute, a non-profit focused on small business supply chain security, and served as CEO of Liberty Group Ventures, LLC. Ms. Todt is a strategic advisor to venture capital firms and serves on Boards of technology companies, which are focused on open-source software, memory safe language, and neurodiversity. She frequently contributes to national television, radio, and print media outlets. She holds a bachelor's degree in public policy from Princeton University and a master's in public policy from Harvard University.



Peter Kant

Chairman and CEO at Enabled Intelligence

Peter Kant is the Founder and CEO of Enabled Intelligence, Inc, an artificial intelligence technology company providing accurate data labeling and AI technology development for U.S. defense and intelligence agencies while providing meaningful high-tech employment to veterans and neurodiverse professionals. Peter has two decades of experience at the nexus of business, government, technology and policy including leadership positions in state and federal government, large companies, start-ups, and technology research non-profits. He also currently serves on multiple corporate and advisory boards of companies and investment funds. Peter started his career in government service working in political positions at the state and federal levels. He worked in the U.S. Congress; served as Policy Director for the Texas House of Representatives; and served as an appointee in President Clinton's administration.



Ann Cleaveland

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

Ann Cleaveland is the Executive Director of the Center for Long-Term Cybersecurity, a multidisciplinary research center at the University of California, Berkeley. She also chairs the Consortium of Cybersecurity Clinics, which she co-founded in 2021. Under Ann's leadership, the Center was chosen to receive the Chancellor's Award for Research in the Public Interest 2022. Ann is also the recipient of American University's 2024 Inclusive Technology Policy Changemaker Award. Cleaveland has held leadership positions in philanthropy, non-profit management, and industry. She previously served as Interim Executive Director of the Berkeley Institute for Data Science and as the Senior Director of Strategic Planning at the ClimateWorks Foundation. She received an MBA in Sustainable Management from the Presidio Graduate School and a B.A. from Rice University. Her research interests include cybersecurity futures, digital risk communications, governance of cyber risk, and secure clean energy.

SPEAKERS



Johan Gerber

Executive Vice President and Head of Security Solutions at Mastercard

Johan Gerber is Executive Vice President of Security Solutions at Mastercard and 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 threats, including cyber, financial crime and fraud. During a career spanning 25 years Johan has overseen the growth of Mastercard's cybersecurity offering, overseeing the successful acquisition of several security tech companies 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.



Natalia Oropeza

Global Chief Cybersecurity Officer at Siemens

Ms. Oropeza is an experienced manager in the area of information technology, whose career includes several leadership roles. She was born in Puebla, where she obtained an electronic engineering degree at the Universidad de las Americas Puebla. She began her career at Volkswagen de Mexico. During her career at VW Group, she was promoted to Chief Information Security Officer for the entire Volkswagen Group and led the company's largest IT transformational program. Currently, as Global Chief Cybersecurity Officer at Siemens, Ms. Oropeza leads a team of more than 1,300 cybersecurity experts. Since 2023, Natalia Oropeza has been the Chairwoman of the Charter of Trust, an initiative with currently 12 partners, including major players like Allianz, IBM or Microsoft, leading efforts to promote cybersecurity and digital trust on a global scale. In addition to her extensive experience in information technology, she holds an MBA in finance and the upper management certification from the European School of Management. Besides her cybersecurity responsibilities at Siemens, she also holds the role of Chief Diversity, Inclusion & Equity Officer. She champions all forms of diversity and leads the global effort to make Siemens an even more inclusive workplace, where every individual feels they belong and has equal opportunities to succeed.



Catherine De Bolle

Executive Director of Europol

Catherine De Bolle has been the Executive Director of Europol, the European Union agency responsible for coordinating law enforcement and combating cross-border crime, since 2018. In her role, she leads Europol in its mission to ensure the safety of EU citizens by promoting information exchange and cooperation between police forces in Member States. Before taking up her position as Director of Europol in May 2018, Catherine De Bolle was Commissioner General of the Belgian Federal Police from 2012 to 2018. Before her appointment as Commissioner General, Mrs. De Bolle was Chief of Police of the local police zone Ninove. In January 2015 she received the title of Public Manager of the Year. From November 2015 to November 2018, she was a member of the Interpol Executive Committee. Mrs. De Bolle studied law at Ghent University and subsequently graduated from the Royal Gendarmerie Academy in Belgium.

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. He has served as the lead lawyer advising on the legal response to operationally impactful malware for many Fortune 500 entities, and led the incident response, associated investigations and litigations for companies impacted by almost every significant global cybersecurity incident. He has earned numerous acknowledgements, including a Band 1 ranking in Chambers USA and Chambers Global for Privacy & Data Security: Incident Response and "Hall of Fame" recognition in Legal 500 for Cyber Law. Mr. Lashway is fluent in several key languages to national security work and is a sought-after speaker on such matters.



Lisa O. Monaco

Former U.S. Deputy Attorney General

Lisa Monaco is a national security and law enforcement leader who most recently served as the 39th Deputy Attorney General of the United States. As the second-ranking official and Chief Operating Officer, she was responsible for overall supervision of the 115,000 person Justice Department; its litigating and policy components, U.S. Attorneys and five law enforcement agencies, including the FBI, reported to her. A veteran of the Justice Department, she served as a career federal prosecutor and in several prior leadership roles. Today, she is a Distinguished Scholar in Residence at New York University School of Law. From 2013-2017, Monaco was Homeland Security and Counterterrorism Advisor and Deputy National Security Advisor to President Barack Obama. She coordinated policy and response to international and domestic terror incidents, cyber threats, pandemics, and natural disasters. She advised the President on all aspects of counterterrorism policy and strategy. Out of government, Monaco has served in private practice and taught national security law. She is a founding co-chair of the Aspen Institute Cyber Group and has served on numerous national security-focused boards and commissions. Born and raised in Massachusetts, she is a graduate of Harvard University and the University of Chicago Law School.



Carsten Meywirth

Head of the Cybercrime Unit, Federal Criminal Police Office (BKA)

Carsten Meywirth ist der Leiter der Abteilung Cybercrime im Bundeskriminalamt. Nach seiner polizeilichen Ausbildung bei der Schutzpolizei des Landes Niedersachsen trat er 1987 in das Bundeskriminalamt ein. Ferner leitete er ab 2005 in der Abteilung Informationstechnik des Bundeskriminalamts unterschiedliche Projekte und war ab 2008 Leiter des Stabes des IT-Direktors. In seiner mehr als dreißigjährigen Amtszugehörigkeit hatte Herr Meywirth in unterschiedlichen Verwendungen in den Abteilungen Zentrale Dienste und Organisierte und Allgemeine Kriminalität Führungsaufgaben übernommen. Im Oktober 2019 wurde er mit der Leitung der Projektgruppe zum Aufbau der Abteilung Cybercrime beauftragt, die zum 01. April 2020 im Bundeskriminalamt eingerichtet wurde. Darüber hinaus leitete er für drei Jahre die Gruppe Cybercrime in der Abteilung Organisierte und Schwere Kriminalität und ab 2016 die Gruppe Zentrale Logistikaufgaben in der Abteilung Zentrale Verwaltung.

SPEAKERS



Sandra Joyce

Vice President Google Threat Intelligence Group

Sandra is a cybersecurity leader with 26 years of intelligence experience. She leads Google Threat Intelligence Group and joined Google in 2022, following Google's acquisition of Mandiant. Sandra is a U.S. Air Force Reserve officer and serves as a faculty member and on the Board of Visitors at the National Intelligence University. She is a member 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 is also a visiting fellow at the National Security Institute, and 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.



Edvardas Šileris

Head of Cybercrime Centre Europol, Netherlands

Edvardas commenced as Head of the European Cybercrime Centre in 2020. He is responsible for the central collation of criminal intelligence on cybercrime across the EU, supporting member state investigations into online child sexual exploitation, cyber-dependent crimes, non-cash means of payment fraud, and crime on the dark web. His Centre collaborates closely with the Joint Cybercrime Action Taskforce (J-CAT), a team of specialist cyber investigators from various countries. His teams at EC3 further provide digital forensic support in complex cases, strategic analysis of threats and trends, liaison with industry, academia and non-law enforcement partners, prevention and awareness, and capacity building. Before becoming Head of EC3, Edvardas was Deputy Police Commissioner General of the Lithuanian Police, also covering innovation, with 22 years dedicated to crime investigation.



Dmitri Alperovitch

Co-Founder and Executive Chairman of Silverado Policy Accelerator

Dmitri Alperovitch is the Co-Founder and Chairman of Silverado Policy Accelerator, a non-profit focused on advancing American prosperity and global leadership in the 21st century and beyond. He is a Co-Founder and former CTO of CrowdStrike Inc., a leading cybersecurity company. A renowned cybersecurity visionary, business executive, and thought leader on geopolitics, great power competition and cybersecurity strategy, Alperovitch has served as special advisor to the Department of Defense and currently serves on the Department of Homeland Security Advisory Council and the Cybersecurity and Infrastructure Security Agency's Cyber Safety Review Board. In 2021, he launched the Alperovitch Institute for Cybersecurity Studies at Johns Hopkins University's School of Advanced International Studies (SAIS).

SPEAKERS



David Sanger

White House and National Security Correspondent,
The New York Times

David E. Sanger is a White House and national security correspondent and senior writer for The New York Times. In his 43-year career, he has been on three Pulitzer Prize-winning teams, most recently in 2017 for reporting on Russian interference in the 2016 election. He has also received numerous journalism awards for his foreign correspondence and national security coverage. Sanger's latest book, *New Cold Wars: China's Rise, Russia's Invasion and the Struggle to Defend the West* (2024), is a New York Times bestseller. He previously authored *The Perfect Weapon*, *The Inheritance*, and *Confront and Conceal*, all bestsellers on foreign policy and national security. *The Perfect Weapon* also became an HBO documentary, as did *Year One*, which examined the Biden administration and the lead-up to the Ukraine war. At The Times, Sanger has held roles including Tokyo bureau chief and chief Washington correspondent, covering five U.S. presidents. He co-teaches "Central Challenges in American National Security, Strategy and the Press" at Harvard's Kennedy School of Government and is a non-resident fellow at the Belfer Center.



Anne Neuberger

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

Anne Neuberger served as Deputy National Security Advisor for Cyber and Emerging Technologies in the Biden Administration. In that role, she was a primary author of multiple Executive Orders and National Security Memoranda on national cyber and technology policy. She also initiated and led the Counter Ransomware Initiative, a 71-nation partnership to combat transnational cyber threats and money laundering via cryptocurrencies. Ms. Neuberger also designed the U.S. Cyber Trust Mark program, a transformative public-private partnership to improve the cybersecurity of connected consumer devices and launched a joint roadmap with the European Union for mutual recognition of cybersecurity labeling. Prior to the White House, she served for over a decade at the National Security Agency (NSA) and the Pentagon in senior operational roles. At NSA, she was appointed deputy director of global intelligence operations (10,000+ professionals). Ms. Neuberger also established and led the Cybersecurity Directorate (4,000+ people). In 2013, she was appointed NSA's first Chief Risk Officer. Prior to government, Ms. Neuberger led technology and operations at a large financial services firm. Throughout her government and private sector roles, she continued to devote significant effort to transformative non-profit projects. Ms. Neuberger received an MBA and Master of International Affairs from Columbia University.



Sir Julian King

Former EU Commissioner

Sir Julian King was the last U.K. EU Commissioner (2016-19) responsible for security, tech and data issues. Previously he was a diplomat: HM Ambassador to Paris and Dublin, Head of the Northern Ireland Office, DG Economic in the FCO, and served in a number of posts (Brussels, New York, Luxembourg, The Hague, Lisbon) as well as in London. He is currently a specialist partner at Flint Global where he advises clients on political, policy and regulatory issues in the UK & Europe. He is a member of the Advisory Board of the Oxford Internet Institute; a Fellow of RUSI; Board member of CER; ECFR Council; and Governor and member of the Council at Ditchley. Sir Julian studied at the University of Oxford and the École nationale d'administration in Paris.

SPEAKERS



Sasha O'Connell

Senior Director for Cybersecurity Programs at Aspen Digital

Sasha Cohen O'Connell, PhD is the Senior Director for Cybersecurity Programs at Aspen Digital. Dr. O'Connell comes to Aspen from American University where she was an Executive in Residence and Senior Professorial Lecturer teaching U.S. cyber policy at the graduate and undergraduate levels and leading the graduate certificate in cyber policy and management she developed. O'Connell began her career at the FBI where she served most recently as the organization's Chief Policy Advisory, Science and Technology and as the Section Chief of Office of National Policy for the FBI's Deputy Director where she led policy engagement with the National Security Council on a wide breadth of issues. Among other roles, O'Connell ran the FBI's Strategy Management Office where she led implementation of the Balanced Scorecard for the FBI's Director. Upon leaving federal service, Dr. O'Connell was a Director in the National Security Segment of Guidehouse where she led engagements with clients in the homeland/national security space. O'Connell holds a Bachelor of Arts from Barnard College as well as an MPA and Doctorate in Public Administration from American University.



Claudia Plattner

President of the German Federal Office for Information Security (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).



Drew Bagley

Vice President and Counsel for Privacy and Cyber Policy at CrowdStrike

Drew Bagley, Esq. is CrowdStrike's Vice President & Counsel for Privacy and Cyber Policy, responsible for leading CrowdStrike's global data protection initiatives, privacy strategy and policy engagement. Mr. Bagley joined CrowdStrike a decade ago after working in the FBI's Office of General Counsel. He is part of CISA's JCDC, Europol's Advisory Group on Internet Security, the U.S. Department of State's International Digital Economy and Telecommunication Advisory Committee, and the DNS Abuse Institute's Advisory Council. He served on the ICANN CCT Review Team and the President's NSTAC Abuse of Domestic Infrastructure Subcommittee. Mr. Bagley, a former German Chancellor Fellow, teaches at American University and co-hosts the Start Here: Cyber Fundamentals for Policymakers podcast.

SPEAKERS



Pascal Andrei

Senior-Vice President Chief Security Officer at Airbus

Pascal ANDREI has a French state PhD degree in Competitive Intelligence & Security from Paris University after a Mathematics and Physics Masters. He started his career at AEROSPATIALE in 1993 as head of Competitive Intelligence before leading e-business activities in Munich for EADS headquarters. He created and led Aircraft Security within Airbus before becoming Chief Product Security Officer and Executive Expert for all Airbus divisions overseeing all Airbus products (aircraft, helicopters, satellites, launchers...). Pascal ANDREI is currently Airbus SVP Head of Security, leading all Security activities globally for Airbus companywide, with a direct report to Airbus CEO. He plays a very active role in international cooperative efforts to guarantee the overall (Cyber and Physical) security of the commercial aviation industry infrastructure. For this contribution, he was nominated personality of the year in 2015 by the Air Transportation System Security community in Dubai. He is a reservist of the "GIGN" the elite police tactical unit of the French National Gendarmerie and was decorated Knight of the Legion d'Honneur in 2017.



Tobias Gotthardt

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.



Gabriel Mitschke-Collande

Chief Digital Officer at 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 responsible for Group and information security, quality management, and G+D Ventures. Von Mitschke-Collande has successfully implemented digital transformation in various management positions. Von Mitschke-Collande most recently worked as CDO for BayWa AG in Munich. The Group CDO has been with G+D since May 2024. 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.

SPEAKERS



Gerhard Fettweis

Vodafone Chair Professor at Technical University Dresden

Gerhard P. Fettweis, is Vodafone Chair Professor at TU Dresden, Germany. Since 2018 he is also founding Scientific Director & CEO of the Barkhausen Institute. He earned his Ph.D. under H. Meyr at RWTH Aachen (Germany) in 1990. Thereafter he was a postdoc at IBM Research, San Jose, and then joined TCSI, Berkeley, USA. Since 1994 he researches wireless communications and chip design, coordinates 5G++Lab Germany and the German Cluster-for-Future SEMECO. His team spun-out 19 tech startups, and initiated 6 platform entities. Gerhard is member of the German Academy of Sciences (Leopoldina), the German Academy of Engineering (Acatech), the US National Academy of Engineering, and Fellow of IEEE, VDE/ITG, NAI, EURASIP, ITG, WWRF, and DATE. He is active in organizing IEEE conferences.



Michele Mosca

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

Michele Mosca is the CEO and co-founder of evolutionQ, a start-up that provides scalable defense-in-depth with post-quantum cryptography (PQC) and quantum key distribution (QKD) software solutions for cryptographic resilience and quantum-safe security. Michele is a renowned expert in cryptography and among the world's leading experts at the intersection of quantum computing and cybersecurity. He has been instrumental in working with the business community to share the importance of cryptography as a critical cybersecurity control protecting both data and communications. Prior to evolutionQ, Michele was a founder of the world-leading Institute for Quantum Computing, a Professor in the Department of Combinatorics & Optimization at the University of Waterloo, and a founding member of the Perimeter Institute for Theoretical Physics. His work on quantum computing has been published widely in top journals and textbooks. Michele worked on cryptography during his BMath (Waterloo) and MSc (Oxford) and obtained his Doctorate (Oxford) in Quantum Computer Algorithms. He was appointed as a Knight in the Order of Merit by the Government of Italy in 2018. The Knighthood recognizes Michele's contributions in quantum information science and digital security, as well as teaching and outreach.



Jacky Fox

Global Cyber Security Strategy Practice Lead, Accenture

Jacky Fox is a Senior Managing Director. She has 20+ years' experience in technology and cyber security consulting. Jacky holds an MSc in Digital investigations and Forensic computing, a GCFA and a GICSP. She has worked across multiple industry sectors including public sector and financial services. Jacky specializes in helping organizations to understand and treat their cyber risk and has had the experience of investigating many national and international breaches. She is also Vice-chair on the board of CyberIreland and is an adjunct lecturer for UCD on their MSc in forensics and security. In 2018, she was awarded 'Security Champion of the Year' in Ireland for her contribution to the Irish security industry and her mentorship and encouragement of women in security.

SPEAKERS



Thomas Saueressig

Board Member of SAP

Thomas Saueressig is a member of the Executive Board of SAP SE. He heads the Customer Services & Delivery Board area with global responsibility for long-term customer value in the cloud. This includes all business areas in customer services, comprising professional services, premium engagements, customer innovation services, and customer support. In addition, Saueressig leads cloud infrastructure, cloud operations, cloud lifecycle management, and private cloud delivery for SAP's global customer base. Previously, as a member of the Executive Board, Saueressig led the SAP Product Engineering Board area and was responsible for the company's entire application portfolio. Before being appointed the head of SAP Product Engineering, he was chief information officer (CIO) and global head of IT Services at SAP. As CIO, he was responsible for SAP's IT strategy and execution following a cloud-first approach. Saueressig has a degree in Business Information Technology from the University of Cooperative Education in Mannheim (Germany) and a joint executive MBA from ESSEC Business School (France) and Mannheim Business School (Germany). Since April 2022, Saueressig has been a member of the Board of Directors of Nokia.



Eva Maydell

Member of the European Parliament

Eva Maydell has represented Bulgaria's GERB and the European People's Party in the European Parliament since July 2014. She is a member of the Committee on Industry, Research and Energy (ITRE) and participates in trade delegations to Japan and the United States. Additionally, she serves as a substitute member of the Committee on Economic and Monetary Affairs (ECON). In 2017, she was elected President of the European Movement International. Eva Maydell is also the Coordinator of the Young Members' Network of the EPP Group, a vice-president of SME Europe, and the initiator and co-founder of Education Bulgaria 2030. Eva Maydell was reelected to the European Parliament in 2019, where she continues to serve on the ECON and ITRE committees, as well as the Delegation for relations with Japan and the Delegation for relations with the United States. In 2020, she was appointed EPP Group rapporteur on the New European Data Strategy and serves as the EPP Group Coordinator/ Speaker in the Special Committee on Artificial Intelligence in the Digital Age. Maydell is also a key member of the Young Members Network of the EPP Group and co-chairs the European Parliament Digital and AI Intergroup. As of April 2024, she was highlighted as one of the MEPs to watch ahead of the 2024 European Parliament elections and is considered a potential candidate for Bulgaria's next commissioner.



Ralf Wintergerst

President of Bitkom, Group CEO of Giesecke+Devrient

Dr. Ralf Wintergerst is Chairman of the Management Board of Giesecke+Devrient (G+D). In addition to his duties as Group CEO, he is responsible for the central areas of Corporate Strategy and Development, Mergers & Acquisitions, Corporate Communications, Compliance Management and Auditing, Data Protection, and Legal and Corporate Governance. As the company's Labour Director, he is also responsible for Human Resources. Alongside his role at G+D, Wintergerst is President of the German digital association Bitkom with more than 2,200 member companies as well as Vice President of the Federation of German Industries (BDI). Furthermore, he is Chairman of the Supervisory Board of secunet Security Networks AG (Essen, Germany). Wintergerst studied business administration and holds two master's degrees – one in management and the other in politics philosophy and economics (PPE). He earned his doctorate at Ludwig-Maximilians-Universität Munich with a thesis on corporate governance and management.

SPEAKERS



Nandan Nilekani

Co-Founder and Chairman of Infosys Limited, India

Nandan M. Nilekani is the Co-Founder and Chairman of Infosys, a leading Indian IT and digital services company with a global presence. He was the Founding Chairman of the Unique Identification Authority of India (UIDAI) from 2009-2014, where he led the creation of Aadhaar, a unique identification system that streamlined access to government services, reduced fraud, and improved delivery of benefits in India. He is also the co-founder and Chairman of EkStep Foundation, a non-profit focused on improving literacy and numeracy in India. In January 2023, Nandan was appointed co-chair of the G20 Task Force on Digital Public Infrastructure for Economic Transformation. Nandan has received numerous accolades, including being named "Asia's Businessman of the Year" by Fortune in 2003 and receiving the Padma Bhushan in 2006. He has been listed among Time's 100 Most Influential People (2006, 2009) and received the Lifetime Achievement Award from E&Y in 2017. Nandan was featured in Time's 100 Most Influential People in AI in 2024 and has authored several books, including *Imagining India* and *Rebooting India*.



Andrea Rigoni

Global Health and Public Sector Group Lead at Accenture

Andrea Rigoni is a Managing Director at Accenture, where he serves as the Global Cyber Security Lead for Healthcare and Public Services and heads the Accenture Secure AI Lab in Brussels. Prior to this, he was a Senior Partner at Deloitte, leading Global Cyber Initiatives in Government and Public Services. Over the years, he has played a pivotal role in shaping national and international cybersecurity policies. He served as Digital Security Advisor to the Italian Prime Minister, co-authoring the Italian National Cybersecurity Strategy, and was Director General of the Global Cyber Security Centre in Rome, focusing on cybersecurity policy and education. Rigoni has also contributed to UN-ITU cybersecurity guidelines and co-authored several publications on cyber defense. Additionally, he served NATO as an External Director to the Science for Peace and Security Division, leading cybersecurity projects in Ukraine, Georgia, and Jordan.



Michael Vetter

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

Lieutenant General Michael Vetter is the Director General for Cyber/IT and Chief Information Officer in the German Ministry of Defence in Berlin since April 2019. Lieutenant General Vetter joined the Luftwaffe as an officer cadet in 1982. From 2012 until 2017 he commanded the Bundeswehr Logistics Centre located in Wilhelmshaven. In 2017 he became the first Vice Chief Bundeswehr Cyber and Information Domain Service (CIDS) and the Chief of Staff CIDS Headquarters. He is a member of the Royal College of Defence Studies in London and a graduate from the Defence Resources Management Institute/United States Navy Postgraduate School in Monterey/California. Lieutenant General Vetter is married to Yasmin. They have six children.

SPEAKERS



Hannah Neumann

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

Dr. Hannah Neumann Member of the European Parliament since 2019, representing "The Greens/European Free Alliance". She serves as the spokesperson for foreign and security policy for her group. She is the coordinator in the Committee on Foreign Affairs (AFET), a member of the Committee on Security and Defence (SEDE), and a substitute member in the Committees on Human Rights (DROI) and Civil Liberties, Justice and Home Affairs (LIBE). She also chairs the Delegation for Relations with Iran (D-IR) and is a member of the Delegations for Relations with Iraq (D-IQ), Afghanistan (D-AF), and the Arabian Peninsula (DARP). Prior to her role in the European Parliament, Dr. Neumann worked extensively in the fields of peacebuilding and political communication. She holds a PhD in Peace and Conflict Studies from Freie Universität Berlin, where she led research projects on post-conflict reconstruction in Liberia and the Philippines. She previously served as a policy advisor in the German Bundestag, and as a freelance consultant for political communication and international security policy.



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 10 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. Before his current position, Bohlin served as a member of parliament for 12 years, including time as a deputy member on the Justice Committee. He later chaired the Committee on Industry and Trade, where he was responsible for developing new energy policies that later formed the foundation of the current government's energy policy. Bohlin studied law at Uppsala University. He lives in the county of Dalarna, Sweden, is married, and has two children.



Zac Stenning

Director of Strategy and Assistant Chief at UK Strategic Command

Major General Stenning is Director Strategy/Assistant Chief, UK Strategic Command. In support of the Command, he is responsible for Strategic Plans including Defence Review and Defence Reform implementation; the £8Bn portfolio that delivers capabilities; strategic workforce planning and international liaison. He also fosters the development of Cyber and Special Operations Forces at the 2* level. He has commanded and has experience of unit, Brigade, Divisional, Joint, Coalition, EU and NATO operations. From 2017-2019 he commanded 1 Armoured Infantry Brigade. The Brigade led on experimentation to design and enact, enhanced methods of fighting for the British Army. Most recently he was the Commandant of The Royal Military Academy Sandhurst and Director Leadership British Army. He was Chief of Staff 3rd (UK) Division between 2014-2017. This period included the re-set to warfighting operations and initial deployments of UK Forces to Ukraine and Estonia. As Head of Military Strategy in the UK Ministry of Defence between 2018-2021, he helped shape and deliver the Integrated Defence and Security Review with responsibility for strategic plans for the employment of UK Forces, Special Operations Transformation and the National Aircraft Carrier Policy.

SPEAKERS



Chris Inglis

Former National Cyber Director at The White House, USA

Mr. Inglis is a Visiting Professor at the U.S. Air Force and Naval Academies, a senior advisor to Hakluyt and Company, a senior advisor to Paladin Capital, a member of the AIG, Mitre and Huntington Bancshares Boards, the US Navy Science and Technology Board, and the U.S. Cybersecurity and Infrastructure Agency Advisory Council. From 2021 to 2023 Mr. Inglis served as the inaugural White House U.S. National Cyber Director, after service as a Commissioner on the U.S. Cyberspace Solarium Commission, eight years as the National Security Agency Deputy Director and Chief Operating Officer (2006-2014) and three years as the Special U.S. Liaison to London. Mr. Inglis holds degrees in engineering and computer science from Columbia University, the Johns Hopkins University, the George Washington University, and an honorary doctorate from the National Intelligence University. Mr. Inglis holds a rating as a US Air Force command pilot and attained the rank of Brigadier General in his active/reserve service.



Oliver Rolofs

Co-Founder of MCSC & Founder and Managing Partner of 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.



Despina Spanou

Principal Adviser in the European Commission for Cybersecurity Coordination

Despina Spanou is Principal Adviser to the Director-General of the Directorate-General for Communications Network, Content and Technology (DG CONNECT) of the European Commission. Prior to that, she was the Head of the Cabinet of the Vice-President of the European Commission, Margaritis Schinas (2019-2024). In this capacity she coordinated the Vice-President's work on security, migration and asylum, health, skills, education, culture and sports. She also coordinated the Vice-President's EU Security Union work, ranging from counterterrorism, organised crime and cybersecurity to hybrid threats. Previously, she was Director for Digital Society, Trust and Cybersecurity at DG CONNECT of the European Commission. Ms Spanou was responsible for the European Union's cybersecurity policy and law, served as a member of the management board of ENISA, and of the Steering Board of the Computer Emergency Response Team for the EU Institutions (CERT-EU). She is a founding member of the Women4Cyber initiative and advocate for the need for more cybersecurity experts in Europe. She also teaches EU Cybersecurity policy at Harvard Kennedy School. Before joining the European Commission, she practised EU competition and trade law with a US law firm for a number of years. Despina Spanou is a member of the Athens Bar Association and holds a Ph.D. in European law from the University of Cambridge.

SPEAKERS



Rolf Schumann

Co-CEO of Schwarz Digits, Germany

Rolf Schumann is Co-CEO of Schwarz Digits, the IT and digital division of the Schwarz Group. Schwarz Digits offers digital products and services relating to cyber security, cloud and artificial intelligence that meet the high German data protection standards - for the greatest possible digital sovereignty. In addition, Rolf Schumann is responsible for the digital activities of the Schwarz Group companies with a focus on e-commerce, loyalty, retail media and digital innovations. With over 30 years of experience in the strategic planning of IT projects and digital transformation, he is constantly driving technology and innovation-related topics across all industries. Before joining the Schwarz Group, Rolf Schumann worked at SAP as General Manager worldwide for the Platform & Innovation division. From 2008 to 2012, Rolf Schumann dedicated himself to the topic of clean tech and founded the start-up company Better Place, with a focus on electromobility. Prior to that, he was CTO for Europe at SAP. Before joining SAP in 2000, Mr. Schumann spent nine years at Siemens, where he was responsible for data center operations in Europe and the planning of Internet architecture.



Volodymyr Lutchenko

CTO of Ukraine's largest mobile operator

As CTO of Ukraine's largest mobile operator, Lutchenko has worked tirelessly to overcome difficult technical challenges during the past ten months of the war time, while Kyivstar has launched several initiatives dedicated to protecting its telco network from destructions and energy blackouts and helping the people of Ukraine maintain access to communications and digital services through their mobile devices. Volodymyr Lutchenko has been named Network X's Telco Executive of the Year 2022, as voted for by his telco peers.



Audrey Tang

Cyber Ambassador and former Minister of Digital Affairs, Taiwan

Audrey Tang is Taiwan's Cyber Ambassador-at-Large and served as the first Minister of Digital Affairs. Tang played a crucial role in shaping g0v (gov-zero), one of the most prominent civic tech movements worldwide. In 2014, she helped broadcast the demands of Sunflower Movement activists, and worked to resolve conflicts during a three-week occupation of Taiwan's Legislature. Tang helped develop participatory democracy platforms such as vTaiwan and Join, bringing civic innovation into the public sector through initiatives like the Presidential Hackathon and Ideathon. Other accomplishments for Tang include shaping Taiwan's internationally acclaimed COVID-19 response, as well as safeguarding the country's 2024 presidential and legislative elections from cyber interference.

SPEAKERS



Stormy-Annika Mildner

Executive Director Aspen Institute Germany

In January 2021, Dr. Stormy-Annika Mildner (M.Sc.) became Director of the Aspen Institute Germany in Berlin. From 2014 to 2020, she served as head of the department "External Economic Policy" at the Federation of German Industries (BDI), where she was responsible for international trade and investment issues. Prior to joining BDI, she was Member of the Board of the German Institute for International and Security Affairs (SWP). She earned a Master of Science in international political economy from the London School of Economics and a PhD in economics from Freie Universität Berlin.



Hanno Pevkur

Minister of Defence of the Republic of Estonia

Hanno Pevkur assumed office as the Minister of Defence of the Republic of Estonia on 18 July 2022. Prior to that, he was a member of the 13th and 14th Riigikogu from 2016 to 2022 and has held several ministerial positions: Minister of the Interior (2014-2016), Minister of Justice (2012-2014), and Minister of Social Affairs (responsible for the fields of work, health, and social protection). Having started his career in law, he went on to serve in the Nõmme District Administration in Tallinn in 2000-2005, first as an administrative secretary and later as city district elder. In 2005-2007, he was a member of the Tallinn City Council, Chairman of the Nõmme District Administrative Board, and an advisor to the Minister of Justice. In 2007-2009, he was a member of the 11th Riigikogu.



Vivian Schiller

VP and Executive Director at The Aspen Digital

Vivian Schiller joined the Aspen Institute in January 2020 as Executive Director of Aspen Digital, which empowers policymakers, civic organizations, companies, and the public to be responsible stewards of technology and media in the service of an informed, just, and equitable world. A longtime executive at the intersection of journalism, media and technology, Schiller has held executive roles at some of the most respected media organizations in the world. Those include: President and CEO of NPR; Global Chair of News at Twitter; General Manager of NYTimes.com; Chief Digital Officer of NBC News; Chief of the Discovery Times Channel, a joint venture of The New York Times and Discovery Communications; and Head of CNN documentary and long form divisions. Documentaries and series produced under her auspices earned multiple honors, including three Peabody Awards, four Alfred I. DuPont-Columbia University Awards, and dozens of Emmys. Schiller is a member of the Council on Foreign Relations; and a Director of the Scott Trust, which owns The Guardian.

SPEAKERS



Lisa Kaplan

Founder & CEO, Alethea

Lisa Kaplan founded Alethea in 2019 to help customers navigate the new digital reality and protect against online risks stemming from disinformation, misinformation, and social media manipulation. Under Kaplan's leadership, the Alethea team has built the scalable technologies and solutions to detect threats to market capitalization and shareholder value, customer bases, physical safety, business operations, and brand and reputation. This includes exposing foreign, domestic extremist, and for-profit disinformation networks that have targeted organizations, institutions, and Fortune 1000 companies. Kaplan has briefed US, NATO, EU, and G-7 policymakers and officials on disinformation. She writes for Brookings and Lawfare, and is frequently sought out by top-tier media outlets, such as The New York Times, Bloomberg, CNN, and the Washington Post. Alethea was named one of the hottest cybersecurity startups to watch in 2023 by Fortune and Business Insider. She was named by the Forbes Technology Council as one of the Cyber Security Founders to watch in 2025; to Inc.'s 2024 Female Founders List for innovative entrepreneurs; PRWeek's 2023 40 Under 40 list for rising stars in strategic and crisis communications; and the 2021 Forbes 30 Under 30 list of top entrepreneurs and leaders. Kaplan is a graduate of Colby College.



Ginny Badanes

General Manager of Democracy Forward at Microsoft

Ginny Badanes is general manager of Democracy Forward, an initiative within Microsoft's Technology and Corporate Responsibility organization that focuses on addressing ongoing challenges to the stability of democracies globally. The initiative includes efforts to protect elections, political parties, campaigns, and NGOs from cyber-enabled threats. The Democracy Forward team also leads Microsoft's work to improve the information ecosystem, which involves combating disinformation, expanding news distribution, increasing media literacy, and working with community-based programs and newsrooms to use technology to expand their reach. Badanes has spent her career at the intersection of politics and technology. Before joining Microsoft in 2014, she was Vice President of political services at CMDI, where she advised presidential and senate campaigns in their efforts to leverage data and technology to improve their finance and treasury operations. Ginny was named to Washingtonian's 2021 and 2022 "Most Influential People" list for national security and defense. She is a graduate of Duke University.



Maia Mazurkiewicz

CEO of PZU Foundation & Co-Founder of Alliance4Europe

CEO of PZU Foundation, Co-founder of Alliance4Europe and host of TV show Anatomy of Disinformation. Maia is an expert on countering disinformation and behavioral changes. She has 15 years of experience in political management, foreign affairs, and communication in administration, business and CSOs. She is a speaker, trainer and moderator. She believes that we need to change the way we communicate, to introduce more understanding in between humans. Maia is a barrister educated in Poland and the United States. Maia founded and cooperated with number of foundations and NGOs where she worked on various projects concerning democratization and political parties trainings in Eastern Europe. She advises clients on strategy building and public affairs, as well as trains on leadership, project management and campaign building. 2011-2015 she has worked in the Chancellery of the President of the Republic of Poland, where she was responsible for transatlantic and European relations.

SPEAKERS



Nicola Hudson

Partner and Cybersecurity,
Data & Privacy Global Lead at Brunswick Group

Nicola joined Brunswick as a Partner in the Cybersecurity, Data & Privacy practice in 2022. She has worked on hundreds of cyber security incidents and has deep expertise in cybersecurity issues and crisis management across both the public and private sector. Prior to joining Brunswick, she was a member of the Executive Board at GCHQ and Director of Policy at the National Cyber Security Centre, having joined the centre as one of the founding Directors in 2016. Previous to this, she was the Head of the UK Prime Minister's Office, managing day-to-day business during a period of 2 referendums and 2 general elections. Her other government role was as Head of Government Strategic Communications for the Government Olympic Committee. Before joining government, Nicola was Head of Communications at the business risk consultancy Control Risks Group and before this Head of Government Relations at Camelot during licence renewal. Nicola brings a wealth of experience in crisis and reputational management, having coordinated the cyber communications response for FTSE250, NYSE, and NASDAQ-listed companies and critical infrastructure across a broad range of sectors and geographies.



Vilas S. Dhar

President at Patrick J. McGovern Foundation

Vilas Dhar is a global expert on artificial intelligence (AI) policy and a champion for equity in a tech-driven world. He serves as President and Trustee of the Patrick J. McGovern Foundation, a \$1.5 billion philanthropy advancing AI and data solutions for a sustainable and equitable future. Appointed by UN Secretary-General António Guterres to the High-Level Advisory Body on AI, Vilas is also the U.S. Government Nominated Expert to the Global Partnership on AI. He serves on the OECD Expert Working Group on AI Futures, the Global Future Council on AI at the World Economic Forum, and Stanford's Advisory Council on Human-Centered AI. He is Chair of the Center for Trustworthy Technology. His LinkedIn Learning course, Ethics in the Age of Generative AI, is the most-viewed AI ethics course globally, reaching over 300,000 learners. Vilas holds a J.D. from NYU School of Law, an M.P.A. from Harvard Kennedy School, dual Bachelor's degrees in Biomedical Engineering and Computer Science from the University of Illinois, and is pursuing doctoral studies at the University of Birmingham.



Alexander Evans

Associate Dean, London School of Economics

Alexander Evans is Associate Dean of the School of Public Policy and a Professor in Practice in Public Policy at the London School of Economics. He directs the MPA in Data Science for Public Policy and teaches courses on technology and geopolitics. A career British diplomat, he formerly worked as an Adviser to the Prime Minister in 10 Downing Street, Strategy Director in the Cabinet Office, and Director Cyber in the Foreign Office. He has served overseas as Deputy and Acting High Commissioner to India and briefly to Pakistan, led a U.N. Security Council expert mission in New York, and worked for the U.S. Department of State in Washington DC. He is a non-executive director of the Internet Watch Foundation. He has previously been an academic at Yale, Nuffield College Oxford and the Henry Kissinger Chair in Foreign Policy at the Library of Congress. He leads a new LSE initiative on regulatory diplomacy and cybersecurity established in 2024.

SPEAKERS



Dennis-Kenji Kipker

Research Director at Cyber Intelligence Institute

Prof. Dr. Dennis-Kenji Kipker is one of the leading minds in cyber security and works as Scientific Director of the [cyberintelligence.institute](https://www.cyberintelligence.institute) in Frankfurt am Main, Member of the Board of Directors of the strategy consulting company CERTAVO AG and Visiting Professor at the private Riga Graduate School of Law in Latvia. Here he conducts research on topics at the interface of law and technology in cyber security, corporate strategy and digital resilience in the context of global crises, with a particular focus on Chinese and US IT law. Kipker is an advisor to the German Federal Government and the European Commission and a member of the Advisory Board of the Lithuanian cybersecurity unicorn NordVPN, the Munich-based IT security company Myra Security as well as in the BSI cyber security expert group for the space sector. Dennis Kipker works voluntarily for the World Justice Project in the USA and on the Advisory Board of the African Center for Cyberlaw & Cybercrime Prevention (ACCP) at Nelson Mandela University in South Africa.



Axel Deininger

President of ECSO & CEO of secunet Security Networks

Axel Deininger has been on the Management Board of secunet Security Networks AG since January 2018 and took over as CEO in June 2019. In October 2021, Axel Deininger was elected Chairperson of the European Cybersecurity Organisation (ECSO). Before joining secunet, Axel Deininger held various positions at the Munich-based Giesecke+Devrient Group for more than ten years, most recently as Group Senior VP and Head of Division Connectivity & Devices at G+D Mobile Security GmbH. The industrial engineer has also gained many years of management experience from positions at companies such as Siemens AG, Infineon Technologies AG and Samsung Semiconductor Europe GmbH.



Hans de Vries

Chief Cybersecurity and Operations Officer at ENISA

Hans de Vries is the chief cybersecurity and operations officer (COO) at the EU Agency for Cybersecurity (ENISA) as of April 2024. He oversees operational activities and provides strategic guidance to the executive director. He represents ENISA in the NIS Cooperation Group, the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe), and the CSIRTs Network, which includes cybersecurity response teams from EU Member States and CERT-EU. His key focus is supporting NIS2 implementation to strengthen cybersecurity across Europe. Previously, Hans was director of the Dutch National Cyber Security Centre (NCSC-NL) for nearly a decade. He served on ENISA's Management and Executive Boards and played a major role in organizing The Hague's ONE Conference, one of Europe's premier cybersecurity events. Hans has held senior positions at the Dutch General Intelligence Services (AIVD) and the Ministry of the Interior (BZK), overseeing ICT management and operational coordination. He has extensive experience in ICT security at both national and international levels. He holds a law degree from Leiden University and began his career in the private sector before joining the Dutch government in 2002. His work continues to influence cybersecurity policy and operations across Europe.

SPEAKERS



Thomas Rosteck

Division President for Connected Secure Systems
at Infineon Technologies

Thomas Rosteck is Division President for Connected Secure Systems (CSS) at Infineon Technologies. CSS is at the core of the IoT and edge AI, offering secured microcontrollers, wireless connectivity, and security solutions, supporting features ranging from post-quantum-cryptography to secured edge AI and thus addressing the needs of a diverse customer base with easy-to-use, trusted, and scalable systems. With his various responsibilities and management roles within Infineon Technologies' leading security business as well as his participation of Germany's Federal Academy for Security Policy (BAKS) 6-month 'Core Course on Security Policy', Thomas Rosteck has become a respected voice in the industry, shaping the future of cybersecurity and standardization in various fields of technology. Thomas is engaged in driving digitalization and security through various bodies as a senior advisor, including board member at BITKOM (Germany's digital association), member of the Stakeholder Cybersecurity Certification Group (SCCG) of the European Union, member of the board of trustees of the Fraunhofer AISEC Institute as well as member of the board of directors of the Charter of Trust. Prior to joining Infineon in 1999, he worked for Siemens Management Consulting as project leader.



Jason Ruger

CISO at Lenovo

As the Mobile Business Group (MBG) BT/IT Lead and Lenovo Chief Information Security Officer (CISO), Jason is responsible for two functions. For MBG, he runs the technology used to design, manufacture, sell and service Mobile products in all regions. In his CISO role, Jason protects customers, employees and shareholders from an array of cyber-attacks. Jason has over 20 years of cyber security and IT experience at Lenovo, Google, Motorola, and consulting firms. He successfully led companies through some of their largest cyber-attacks in history, and built many aspects of Motorola's modern CRM initiative. Jason holds a Bachelor's degree in Economics from Vanderbilt University and an MBA from Northwestern's Kellogg School of Management. He is based in Chicago.



Jeff Moss

President and Founder of DEF CON

Jeff Moss is the founder of both the Black Hat Briefings and DEF CON conferences. Mr. Moss is a member of the UK Government Cybersecurity Advisory Board (GCAB 2022-). Mr. Moss has been a sworn member of both the DHS Advisory Council (HSAC 2009-2020) and the CISA Advisory Council (CSAC 2021-2025) serving as the chairman of the Technical Advisory Council. Mr. Moss has served as a commissioner on the Global Council on the Stability of Cyberspace (GCSC 2017-2021), was a nonresident Senior Fellow at the Atlantic Council Cyber Statecraft Initiative (2013-2023) and is a member of the Council on Foreign Relations. He is a past CSO of ICANN, was a technical advisor to the TV series "Mr. Robot" and currently lives in Singapore.

SPEAKERS



Perri Adams

Special Assistant to the Director of DARPA

Ms. Perri Adams is a special assistant to the director at DARPA, where she advises stakeholders at the agency and across the U.S. government on the next generation of AI and cybersecurity technology. Prior to this role, Adams was a program manager within DARPA's Information Innovation Office (I2O), where, among other programs, she created the AI Cyber Challenge (AixCC). Previously, she was also a technical advisor for research and development programs at DARPA.



David Weston

Vice President, Enterprise and OS Security at Microsoft

David Weston is the Vice President of enterprise and OS security at Microsoft where he is responsible for the Security engineering of Windows, XBOX, Windows Server, the Azure OS as well as the Offensive Security Research & Engineering Team. Before leading security engineering in Windows, David led security research for Microsoft Defender, detecting and responding to the real-time evolution of the global threat landscape. David has been with Microsoft since Windows 7, holding many different security roles in mitigation design, penetration testing, malware analysis, and threat intelligence. In addition to his engineering work, David is also an accomplished security researcher presenting his work at numerous security conferences including BlueHat, Blackhat, DEF CON and more.



Yan Shoshitaishvili

Assistant 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. Aside from publishing dozens of research papers in top academic venues, Yan led Shellphish's participation in the DARPA Cyber Grand Challenge, achieving the creation of a fully autonomous hacking system that won third place in the competition, and helps guide Shellphish toward the final event of the successor competition, the AI Cyber Challenge.



Bill Woodcock

Secretary General of Packet Clearing House

Bill Woodcock is the secretary general of Packet Clearing House, the intergovernmental treaty organization that builds and supports critical Internet infrastructure, including Internet exchange points and the core of the domain name system. Bill is best known for his work in the 1980s developing the anycast routing technique that now protects the domain name system, and his work establishing Internet exchange points since the 1992. In 2002, he co-founded the INOC-DBA security-coordination hotline communications system that interconnected the network operations centers of more than three thousand ISPs around the world. And in 2007, Bill was one of the two international liaisons deployed by NSP-Sec to the Estonian CERT during the Russian cyber-attack. Now, Bill's work focuses principally on the security and economic stability of critical Internet infrastructure.

SPEAKERS



Linus Neumann

Chaos Computer Club

Linus is a hacker, IT security consultant, and trained psychologist. As a spokesperson for the Chaos Computer Club (CCC), Europe's largest hacker organization, Linus actively identifies, reports, and critiques IT security flaws in critical infrastructures. He has exposed vulnerabilities in Germany's election systems and government-backed communication services and contributes to critical vulnerability disclosures daily. Linus has advised the German Bundestag on multiple iterations of IT security legislation, accurately predicting their repeated failure. He also played a role in the downfall of a German provider of state-sponsored malware, a contribution he takes particular pride in.



Joel Krooswyk

Federal CTO at GitLab

Joel Krooswyk is the Federal CTO at GitLab. Joel's 25 years of leadership experience span not only the US Public Sector, but also small, mid-market, and enterprise businesses globally. Joel combines deep government policy expertise with a wealth of experience in technology, software development, AI, and cybersecurity. He is frequently called upon by industry and agencies alike for policy commentary and response. Joel frequently speaks at major industry conferences on topics such as software development, AI, and cybersecurity and contributes to Public Sector-focused publications, including NextGov, Federal Times, and Federal News Network.



Philip Stupak

Former Assistant National Cyber Director at The White House

Philip Stupak served in President Biden's White House as the Assistant National Cyber Director. He was a senior leader where he created and managed the Policy Implementation Division of the Office of the National Cyber Director (ONCD) to execute President Biden's cybersecurity executive orders, coordinate deployment of the National Cybersecurity Strategy, advance cyber workforce and education initiatives, and harmonize federal cybersecurity policies. He was also responsible for ONCD's partnerships with non-federal stakeholders at the international, state, local, tribal, and territorial levels. Mr. Stupak previously served in President Obama's Administration where he handled cybersecurity and international relations portfolios for the Deputy Secretary of the U.S. Department of Homeland Security. He has a BA from the University of California, Berkeley and a JD from the University of Richmond. He teaches cybersecurity policy at the University of Chicago.



Jacob Braun

Executive Director of the Cyber Policy Initiative, University of Chicago

Jacob (Jake) Braun is the Executive Director of the Cyber Policy Initiative and lecturer at the University of Chicago Harris School of Public Policy. Braun most recently served as the White House acting Principal Deputy National Cyber Director. Before that, he was Senior Counselor for Transformation to the Secretary of Homeland Security, and from 2009 to 2011, Braun was the White House Liaison to the Department of Homeland Security.

SPEAKERS



Christopher Painter

Former President of the Global Forum on Cyber Expertise Foundation

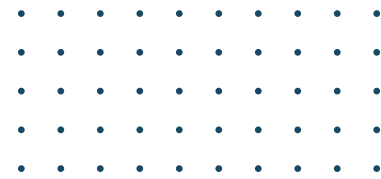
Christopher Painter is a globally recognized leader and expert on cybersecurity and cyber policy, cyber diplomacy and combatting cybercrime. He has been on the vanguard of U.S. and international cyber issues for over thirty years—first as a prosecutor of some of the most high-profile cybercrime cases in the United States, and then as a senior official at the Department of Justice, the FBI, the National Security Council and serving as the world's first dedicated cyber diplomat at the State Department. Among other things, he served as Associate Fellow at Chatham House, a board member of the Center for Internet Security and on the Public Sector Advisory Board for Palo Alto Networks.



Carole House

Former Special Advisor for Cybersecurity at NSC, USA

Carole House is a strategic technology executive and Senior Visiting Scholar at the Georgetown University CyberSMART Center, having recently departed the White House National Security Council (NSC) as Special Advisor for Cybersecurity and Critical Infrastructure and previously serving as the Director for Cybersecurity and Secure Digital Innovation. Carole has held positions in the private sector and on advisory boards for three financial regulatory agencies and two non-profits. Carole's prior government service involved service as a U.S. Army Captain as well as positions leading emerging tech, cybersecurity, and national security initiatives across the White House, Senate Homeland Security Committee, and the U.S. Treasury.



Towards a Secure Digital Era. A Call to Action at the Munich Cyber Security Conference

Around the world, cyber threats are escalating, targeting critical infrastructure, public institutions, and the nonprofit sector. Ransomware attacks, supply chain vulnerabilities, and AI-powered disinformation campaigns have far-reaching implications that transcend borders, jeopardizing societal stability and public trust. Essential services and critical actors, like civil society organizations, are particularly vulnerable yet often lack the resources to defend themselves. How can we collaborate globally to protect these vital organizations and foster a secure, resilient digital future?

CyberPeace Tracer: Illuminating the Threat Landscape for Nonprofits

In response to these growing threats, the CyberPeace Institute is launching the CyberPeace Tracer, the first publicly accessible platform to provide real-time insights into the cyber threats facing civil society. The CyberPeace Tracer is a public platform designed to track and analyze cyber incidents globally, with a focus on nonprofits. The Tracer highlights threat actors, their tactics, attack types, and the impacts and harm of cyberattacks on civil society organisations, while also revealing the broader impact on societal stability and human security.

Its purpose is to:

- Raise public awareness of the cyber threats targeting civil society.
- Equip policy and decision makers with actionable knowledge to improve relevant regulations and thoroughly advocate for sustainable digital resilience driven by evidence.
- Provide timely alerts and actionable intelligence that organizations can use to mitigate risks effectively.
- Advocate for justice by providing data to support legal advocacy efforts, empowering organizations to seek redress and accountability.

The CyberPeace Tracer leverages the CyberPeace Institute's Cyber Harm Methodology to analyze the ripple effects of cyber threats on vulnerable communities. By combining threat intelligence with an alerting service tailored to civil society organisations, the platform delivers actionable insights, timely notifications of emerging threats, and a rapid-response mechanism to connect organizations with volunteer experts for immediate remediation.

It will progressively integrate:

- AI-Powered Cyberattacks: Enhancing awareness and understanding of increasingly sophisticated threats that leverage artificial intelligence for automation, deception, and large-scale exploitation.
- Disinformation Analysis: Integrating insights into disinformation campaigns to highlight how harmful narratives intersect with cyber operations.
- Strategic Reporting: Adding in-depth reports based on dashboard data to identify emerging trends and provide actionable insights for decision-makers.

A Call to Action: Defend The Most Vulnerable to Achieve Digital Resilience for All

At a time when the EU and its allies are reinforcing their collective security against cyber threats, civil society organisations must not be overlooked. Governments, private companies, and civil society must come together to ensure these vulnerable communities are not left to face these digital threats alone. To further improve the platform and enhance digital resilience across civil society, we welcome assistance in a variety of areas, including providing data and insights, offering financial support, sharing stories, reporting incidents, or volunteering.

Together, we can turn the tide against those who seek to exploit the most vulnerable, safeguard societal resilience, and uphold the shared values and human security that define us all—by fostering collaboration, strengthening cyber defenses, and advancing policies that protect people and democratic institutions in the digital age.

Data Partners



Excerpt from the Publication “Cybersecurity Policy Recommendations for the New Administration” of the Aspen Institute’s US Cyber Security Group:

1) Personnel is Policy: Demonstrate Cybersecurity Leadership and Prepare for Immediate Response

Streamline cybersecurity leadership; [...] Redundancies, delayed appointments and vacant political positions can make it hard to develop coordinated and unified strategies, policies and response efforts. [...] Advisors have an opportunity to prioritize, clarify, and align roles to promote efficiency, economies of scale, and maximum impact.

2) Prioritize Cybersecurity Regulatory Alignment and Streamlining

Streamline regulations; there are too many and they are inconsistent. [...] A balance must be struck between centralization and customization in terms of standards and regulation. [...] All new requirements must be rationalized around simple core principles that appropriately balance national security and business interests, including small businesses and local governments. [...]

3) Partner with the Private Sector to Protect Critical Infrastructure and Hold Bad Actors Accountable

[...] Power grids, transportation systems, water supplies, and communication networks are all in jeopardy. You can send a clear message: the United States will defend itself against cyber aggression with the same resolve as it defends against physical threats. Everything from defensive measures to offensive operations should be on the table. Crooks, spies and terrorists should be hunted jointly with key private sector actors. Efforts to “defend forward” must be continued in conjunction with providing resources and assistance to critical, often overlooked

entities such as small businesses and rural communities. [...] We must leverage the U.S.’s unique combination of innovation and capital investment to support and incentivize in areas of the world aligned with U.S. interests.

4) Continue Building Mechanisms to Measure Progress

Government efficiency depends on good data and clear-eyed analysis. We can’t understand what works without data. We need a repository of data in this area to know what to keep and what to cut.

5) Reset the Discussion with Improved Communications Around Cybersecurity Issues

[...] Using the White House bully pulpit is essential [...] In cybersecurity. To move forward quickly, it is imperative to advance a new [...] understanding of cybersecurity from a technology problem for technologists to solve; to an issue of national concern that requires an all-hands-on-deck approach. Cybersecurity must be seen as what it is: 1) a key enabler of economic growth and national security and 2) a critical tool in the effort to counter nation state actors like China.

Full article available at

https://www.aspendigital.org/wp-content/uploads/2025/01/US-Cybersecurity-Group_Cybersecurity-Policy-Recommendations-for-the-New-Administration_January-2025.pdf



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.

Seven Trends Shaping Cyber Threats and Risk Management for 2025



Steve Durbin

Chief Executive of Information Security Forum ISF

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.

The cyber threat landscape has expanded and evolved significantly over these past few years. Attacks have become far more sophisticated, targeted and disruptive and cybercriminals are exploiting vulnerabilities in everything from software to devices to people. Let's understand some of the major trends worth noting in this evolution.

1. The growing interlock between cybersecurity and geopolitical risk

The lines between cybercrime, espionage, and nation-state attacks are blurring. Organized crime syndicates are increasingly operating at least with the tolerance of their host regime, if not the active backing of a nation-state. Critical infrastructure is increasingly vulnerable to cyberattack and state actors are constantly probing for weaknesses. Intelligence agencies are targeting enterprises for intellectual property that could give their nations a military, political, or commercial advantage.

2. The modernization of espionage

If a nation-state actor has the opportunity to impede their adversary, disrupt their national infrastructure, or influence their elections for their country's benefit, will they proceed to take advantage? Of course, they will. This is what can be referred to as the modernization of good old-fashioned espionage. The only difference is that modern spies do not need to lurk around corners, listening through doors. They can sit at their keyboards in plush offices conducting espionage from across the border.

3. The rapid pace of digitalization and birth of new attack vectors

Systems and machines previously built in the analog era are now online and connected, giving cybercriminals plenty of opportunity to disrupt what we now refer to as cyber-physical systems. The rise of technologies like cloud computing, Internet of Things (IoT) and artificial intelligence coupled with trends such as remote work, is not just changing how businesses operate, but it's also changing how adversaries and cybercriminals attack businesses. Quantum computing is also looming on the horizon, a phenomenon that will compel businesses to rethink cybersecurity approaches.

4. A myriad of global challenges

The global cybersecurity industry is struggling with a massive talent shortage. The way data is being transferred across

borders is becoming increasingly complicated due to rapidly evolving data privacy and cybersecurity regulations. Supply chain attacks, where cybercriminals target third-party vendors, software components and service providers, are on the rise. Extortion-based attacks (a.k.a. ransomware) continue to be a challenge. A majority of cyberattacks stem from human error but there is still a general lack of understanding of cybersecurity best practices among employees.

5. The democratization of cybercrime

Organized crime is becoming big business and a lot more accessible to low-skilled players. Unlike in the past, where cybercriminals had to develop their abilities through trial and error, today anyone can simply shop the dark web and buy pre-made phishing kits and platforms like ransomware-as-a-service. Extensive support is provided, including training programs, 24/7 support lines, and a choice of package options. An entire industry catering to cybercrime has been set up.

6. The rise of AI-driven sophistication on attacks

Phishing and social engineering have been around for decades. However, what's changing is that they are becoming a lot more sophisticated and targeted, particularly due to the rise of AI. Deepfakes and human impersonation schemes are being deployed in all sorts of online scams and deceptive social engineering attacks. Disinformation is being weaponized. AI is being used to manipulate facts and distort truth, helping to create polymorphic malware strains that can evade detection by standard security tools.

7. The emergence of threat management as a strategic business priority

Threat management has now become a critical business issue, which wasn't the case five or ten years ago. Board members now understand it, are increasingly accountable for it, and recognize that strong cybersecurity practices must be weaved into corporate strategy. As a result, cybersecurity is no longer viewed as a purely IT or technical issue but as a critical business function that impacts an organization's ability to operate, innovate, and build trust with customers.

What can organizations do to prepare themselves?

Ultimately, technological evolution is what drives cybersecurity evolution. Will we see the threat landscape change and evolve,

become more frequent and intense? Of course we will. Will societies be able to survive an attack on the healthcare system, an attack on the financial system, an attack on the power grid? What can organizations do about it?

It all starts with determining the amount of time your systems can afford to be offline. If there are critical business infrastructure components that cannot tolerate more than a few seconds or minutes of downtime, those are the areas that require immediate and concentrated attention from day one. Cutting corners in this regard is not advisable.

Prioritizing resilience and recovery are essential because achieving 100 percent security is not possible. Attacks can originate unexpectedly and vary in their severity. Rather than attempting to predict future threats, it is more practical to focus on expediting the recovery process and bolstering the resilience of your systems and workforce.

Find out more at

-  www.securityforum.org
-  steve.durbin@securityforum.org
-  <https://www.linkedin.com/in/stevedurbin/>

Threat Horizon 2027

Threat Horizon 2026

Threat Horizon 2025

Threat Horizon 2024

Threat Horizon 2023

Threat Horizon 2022

Threat Horizon 2021

Threat Horizon 2020

Threat Horizon 2019

Threat Horizon 2018

Threat Horizon 2017

Identity underpins every action

Geopolitics impacts every plan

Data sustains every business

Your trusted global risk outlook

Visit securityforum.org to learn more about how your organisation can utilise the ISF Threat Horizon series.

ISF Better Cybersecurity

Find out more

securityforum.org | info@securityforum.org |  Information Security Forum

With a community of over 27,000 information security professionals, we are the recognised authority on cyber, information security and risk management.

©2025 Information Security Forum Limited

Cyber Activity Balance (2022-2024): The EU in Focus



Annegret Bendiek
Senior Fellow at SWP,
Germany

Co-Lead of the Cluster “Cybersecurity and Digital Policy” and Senior Fellow in the EU/Europe Research Division at the German Institute for International and Security Affairs (SWP Berlin). She serves as one of the principal investigators of EuRepoC.



Jakob Bund
Associate at the
German Institute for
International and
Security Affairs (SWP)

Associate at the German Institute for International and Security Affairs (SWP), where he serves as threat intelligence liaison for EuRepoC and editor of the Cyber Conflict Briefing series. Jakob is also a Senior Researcher for Cyber Conflict and Statecraft at Virtual Routes (formerly the European Cyber Conflict Research Initiative (ECCRI)).



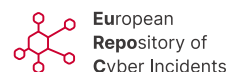
Jonas Hemmelskamp
MA – Chief Data
Scientist for the
EuRepoC project

MA – Chief Data Scientist for the EuRepoC project and a PhD student at the Institute of Political Science, UHEI. He completed his master’s degree in political science at Heidelberg University, where his thesis examined hybrid threat indicators.

The persistent nature of threats enabled by cyber and information space (CIR) capabilities has put the response strategies of governments in Europe and beyond to the test. The cumulative gains cyber campaigns seek to develop challenge traditional diplomatic tools that are designed to impose one-off consequences. To further the understanding of how foreign and security policy instruments can contribute to countering these threats, the European Repository of Cyber Incidents (EuRepoC) has been tracking cyber operations of political implication and state responses for a quarter-century. The trend analysis enabled by this time horizon points to four main developments:

1. For the period since Russia’s large-scale invasion of Ukraine, the Repository has documented 444 politically significant cyber operations against the EU and its member states, conducted by 76 distinct threat actors. A large proportion of this malicious activity directed against EU Member States has targeted government institutions and critical infrastructure vital to the functioning of society, predominantly in the health, transport and financial sectors. The opportunistic targeting of vulnerable organizations by financially motivated actors has led to an increase in operations against organizations providing public goods, in particular in the research and education sectors.
2. Geopolitical shifts translate to the types of operations that actors are choosing to challenge Europe: criminals and Russian state-affiliated groups are mainly targeting state institutions in the EU. China nexus groups have focused on corporate targets and, increasingly, critical infrastructure in the EU.
3. Within the EU, the founding member states are experiencing the highest volume of malicious activity. Public political or diplomatic reactions are also tracked more frequently for this set of states compared to other EU countries. Such public reactions, however, do not regularly lead to official attributions.
4. Attribution time, as a measure for the period between the initial compromise of an organization and public assessments of responsibility, has notably decreased over the last decade. This reduction is in part accounted for by the incentives for hacktivist and ransomware groups to promote and potentially exaggerate their activities to create public pressure on victims. Contributing to this downward trend, however, is also a convergence between attribution timelines of industry and government agencies, indicating closer public-private coordination on the reporting of threat activities.

The full version of this briefing drawing on expanded data analysis, is published in cooperation with Tagesspiegel Background. Available online at:



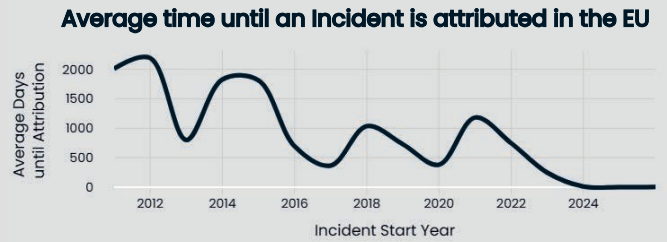
<https://eurepoc.eu/publications/>

Cyber Activity Balance 2022 – 2024: The European Union in Focus

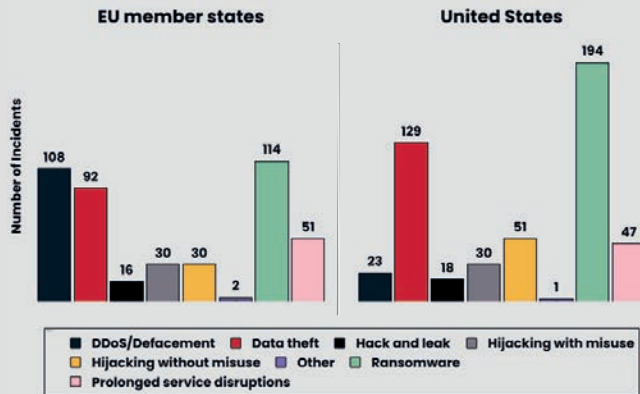
444 incidents documented within the EU

249 incidents affecting critical infrastructure

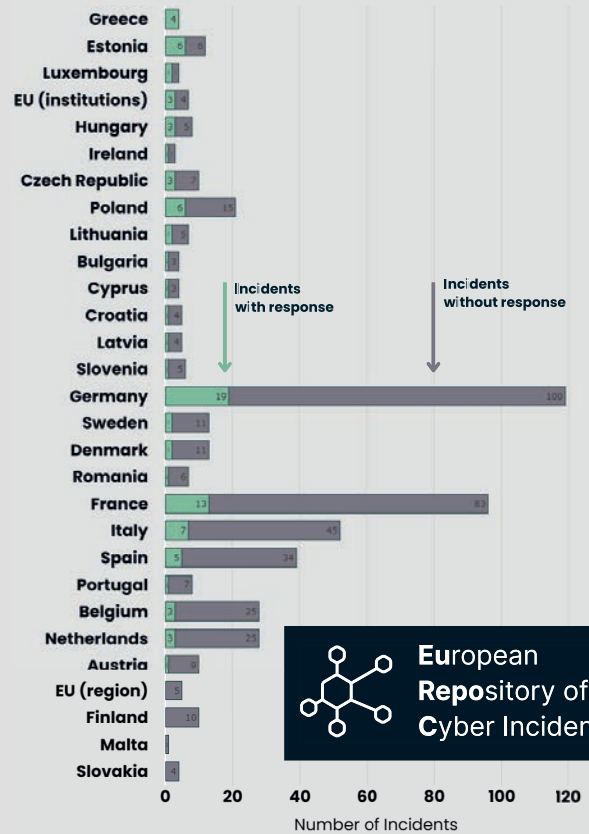
76 active threat actors attributed



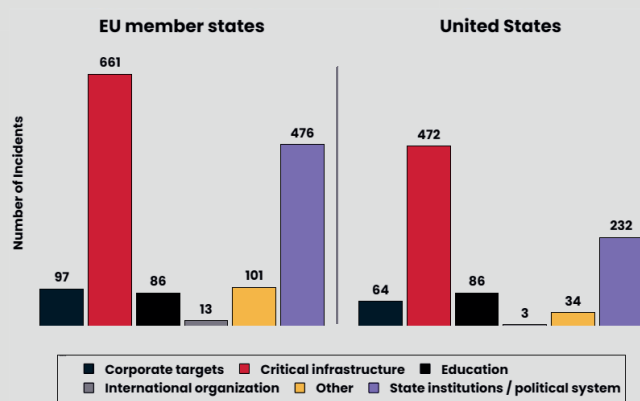
Operation types targeting EU member states/USA



Political response rate for incidents within the EU



Receiver sectors in EU member states/USA



UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386



Stiftung Wissenschaft und Politik
German Institute for International
and Security Affairs



CPI
CYBER POLICY
INSTITUTE

universität
innsbruck

TESTIMONY

Excerpts from the Oral Statement of Kemba Walden to the Committee of Homeland Security



Kemba Walden

President of the Paladin Global Institute and Former Acting U.S. National Cyber Director

I am Kemba Walden, President of Paladin Global Institute and co-chair of Aspen Digital U.S. Cybersecurity Group. I am here today in my personal capacity, drawing from my experience as a former acting National Cyber Director and my roles at Microsoft and the Department of Homeland Security.

The Evolving Threat Landscape

There are two campaigns in the past four years that I hope the Committee will focus its attention on.

The first is the recently uncovered targeting of our Nation's critical infrastructure by the People's Republic of China. This activity, dubbed "Volt Typhoon," represents a step change in the PRC's cyber operational capability, demonstrating their willingness to preposition in our critical infrastructure in preparation for a future conflict.

Second, we've now witnessed the PRC snooping on our telecommunications networks (i.e., Salt Typhoon) Salt Typhoon shows the PRC investments are paying off in a truly scary fashion, as they have accessed the beating heart of the Internet itself.

I raise these two examples to highlight the stakes we face. The PRC's capabilities are rapidly improving, and we have seen from their behavior that they are ready to use cyber tools to attack our critical infrastructure. But, despite these threats, there are key steps that Congress and the new Administration can take to increase our resilience and improve the Nation's cybersecurity posture.

Policy Recommendations

We must strengthen national cybersecurity by clarifying the roles and responsibilities of the private sector and government; upskilling our collective workforce; and embracing technological innovation. On the roles and responsibilities front, there are three legislative items that I would offer as low-hanging fruit for you:

- The Cybersecurity Information Sharing Act of 2015 expires in September. This Committee must take action to reauthorize that legislation to ensure we do not see hard-won progress lost to Congressional inaction. I also urge the Committee to further clarify liability protections related to defensive measures to allow for the most proactive defensive approach possible.

- Regulatory harmonization is an enormous challenge that places an untenable burden on business while harming our cybersecurity. Last Congress, Senator Peters, Senator Lankford, and Congressman Higgins introduced legislation to help bring coherence to the multitude of Federal regulatory approaches by empowering the National Cyber Director. And Congress should move swiftly to reintroduce and advance this important bill.
- This Committee should also work to codify the Cyber Safety Review Board, or CSRB, which helps to understand the root cause of cyber incidents to keep us from making the same mistakes over and over. I hope you will also consider strengthening the board, by making it full-time, independent, and non-partisan with its own administrative subpoena power.

Of course, all the policies in the world are meaningless without the workforce implementing them. While there are several successful programs that are helping to put a dent in the hundreds of thousands of unfilled cyber jobs we have in this country, there is more we can do. To remain sustainable, Congress should expand CISA's current cyber workforce programs; increase the number of internships and apprenticeships available to qualifying students—with or without college degrees; and provide incentives for cyber professionals to work at under-resourced targets like hospitals and water systems.

Finally, I urge you to embrace technology – including from venture-backed companies that are truly at the cutting edge – and allow it to be part of the solution. Supporting the use of artificial intelligence for threat detection and response can help neutralize sophisticated cyber threats more efficiently.

Distinguishing between our digital presence - knowing who's who, and that you are you - is of paramount importance for cybersecurity. The federal government must update its digital identity guidelines to prevent unauthorized access, phishing and email-based attacks, and decrease cyber fraud of public benefit programs.

Conclusion

In conclusion, the global cyber threat landscape requires a coordinated, proactive approach combining legislative action, technological innovation, and operational collaboration. Acting together, we can protect our national security interests while fostering innovation and economic growth.

Thank you again for the opportunity to appear before you. I look forward to your questions.

January 22, 2025

We Need A Transdisciplinary Coalition To Create Responsible AI



Nayef Al-Rodhan

Head of the Geopolitics and Global Futures Department

How do we prepare for a future where the long-term effects of Artificial General Intelligence (AGI), or the more profound Artificial Super Intelligence (ASI), could surpass our current imaginations of what it can do? And how do we deploy AI responsibly without widening inequality and geopolitical insecurity? These questions are at the heart of discussions this week at the Munich Cyber Security Conference.

To unlock the full potential of AI, we must put technology equity and ethical frameworks at the forefront of our thinking. Our current ethical, security and regulatory guidelines are insufficient for a new era of technological disruption. There is a growing disconnect between technological advancement and society's understanding of related moral potholes and risks to our freedoms, civil liberties and dignity needs. To bridge this gap, the world needs a coalition of highly trained transdisciplinary thinkers, including philosophers, political scientists, neuroscientists, anthropologists, social scientists, and AI experts.

Years ago, the futurist Roy Amara famously observed that we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run. We could be guilty of this when it comes to the looming potential of AGI. We're entering an era of radical technological change and yet we're still ill-equipped – logistically, ethically, morally – for the unprecedented technological changes coming our way. This begs an uncomfortable question: how can we truly protect humanity from the potential perils of AI? In a highly connected and deeply interdependent world, disruptive technologies such as AI and synthetic biology can easily create individual and collective dignity deficits, which in turn feed conflict and contempt. We must therefore apply transdisciplinary approaches to make sure that the use and governance of AI is always steered by human dignity needs for all, at all times and under all circumstances. If we ensure that these dignity needs are met, our neurochemically-mediated emotions and motivations are more likely to promote social cohesion and cooperative behaviour. If not, the opposite is likely to happen.

To steer humanity towards a more sustainable and prosperous global order, we must think outside the box and strive towards win-win, multi-sum, absolute gains and non-conflictual competition, embodied by my Symbiotic Realism paradigm. Drawing on

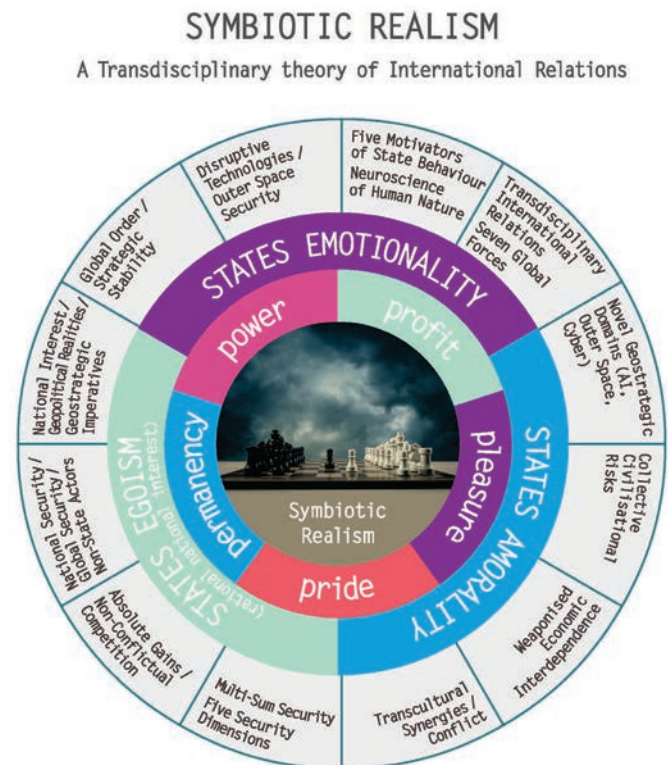
empirical insights from fields such as neuroscience, neurobiology, and neuroimaging, Symbiotic Realism provides a novel transdisciplinary framework. This framework helps analyse how seven interdependent forces shaping the global system influence states behaviour and our relationship with disruptive technological advancements. This nuanced, non-speculative understanding of the predispositions of human nature is increasingly critical, as our innate tendencies profoundly influence how we leverage emerging technologies.

We may not have all the answers about the future potential and trajectory of AI, but transdisciplinary approaches will be invaluable in asking the right questions that will help prepare humanity for what is to come and mitigate the inevitable risks.

Professor Nayef Al-Rodhan is Head of the Geopolitics and Global Futures Department, Geneva Center for Security Policy, and an Honorary Fellow of St. Antony's College, Oxford University. He is also a Member of the Global Future Council on the Future of Complex Risks at the World Economic Forum.



Professor Nayef Al-Rodhan



© Nayef Al-Rodhan 2024

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:



Despina Spanou, Benedikt Franke, Kiersten Todt, Marc Raimondi, Stormy-Annika Mildner, Annegret Bendiek, Benjamin Bögel, Molly Hall, Suntka von Halen, Diana Görlich, Janet Bosshammer, David Lashway, Geoff Brown, Christopher Ahlberg, Jonathan Luff, Monica Todros, Andrea Rigoni, Antonia Schmidt, Christine Skropke, Jennifer Pernau, Tim Maurer, Shyam Mundhada, Jennifer Kaiser-Steiner, Thilo Kräusslich, Ralf Schneider, Andreas Kind, Alexander Schellong, Wolfgang Baare-Schmidt, Tobias Kiesling, Damaris Söllner, Zoey Stambolliu, Maria del Pino González, Paola Arrabal, Detlef Houdeau, Heinz Stiahtny, Michael Tagscherer, Nooshin Soltani, Jamie Cox, Richard Vaerst, Kristina Mader, Konstantinos Ntantonos, Ian-tsing Joseph Dieu, Katharina Bertz, Isabell Weller, Thomas Tarantino, Stefan Lankes, Alexander Wieser, June Chambers, Jens Redmer, Hirokatsu Inoue, Motohiro Tsuchiya, Shinichi Yokohama, Arthur de Liedekerke, Ieva Ilves, Benno Mühler, Kushal Prakash, Ingrid Dickinson, Jordana Siegel, Timo Blenk, Silke Huber-Voigt, Marina Hoffmann, Marina Geigenberger, Christine Schmerber, Kai Hermsen, Paul Desprez, Philip Stupak, Stefan Jost-Dummer, Bernhard Rohleder, Kerstin Petretto, Eda Aygen, Sebastian Doedens, Sandra Proske, Amelie Renken, Matthias Bandemer, Ulrike Strauss, Marcel Lewicki, Susanne Dehmel, Felix Kuhlenkamp, Clemens Schleupner, Valentin Weber, Werner Theiner

This conference was organised by:



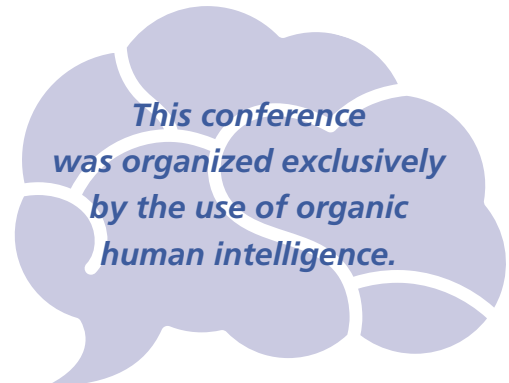
Peter Moehring
Managing Director
Security Network Munich



Charlotte Kobel
Security Network Munich



Rebecca Freyemann
Giesecke+Devrient



Invaluable contributions by:



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



Vivian Schiller
VP and Executive Director at
The Aspen Digital



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



Jeff Moss
Founder of DEF CON



John Mengers
Founder and Executive
Director of C-Suite Advisors

INSTITUTIONAL PARTNERS:

