Security Network Munich

@SN_Munich
#MCSC23

SECURITY NETWORK MUNICH
PRESENTS

MCSC

MUNICH CYBER SECURITY CONFERENCE 2023

Cyber Security: Who is in Charge? – Dealing with Blurred Lines of Responsibility

Chamber of Commerce Munich (IHK)
16/17 February 2023

Patronized by:

Bavarian Ministry of Economic Affairs, Regional Development and Energy

Supported by:

AIRBUS, paloalto NETWORKS, Recorded Future, KSG KREBS STAMOS GROUP, Giesecke+Devrient Creating Confidence, REPLY SPIKE, MYRA Neue digitale Sicherheit, Google, XM Cyber A Schwarz Company, intel, SCHWARZ, LIDL, Kaufland, Infineon, SentinelOne, EY Building a better working world, ALTOPARTNERS Deutschland, SCHWARZ Produktion, prezero

Claudia Eckert

Distinguished Guests,

Welcome to the 10th edition of the Munich Cyber Security Conference which for the first time is taking place at the recently refurbished Seat of the Munich Chamber of Commerce.

One year ago we were still hoping that the conflict which lead to the invasion of Russia into the Ukraine could be defused. This war has shaken the foundations of our continent and beyond, we are facing risks which were not even remotely considered relevant ever since the Iron Curtain came down.

The conference title is Cybersecurity: Who is in charge? It does not only refer to different lines of responsibility and how to find a better understanding in interlinking them for better efficiency in our effort to mitigate cyber risks. It also refers to the fact that there is only One cyberspace and that a military conflict can affect also non-military targets. So we need to rethink our defenses and strategies and perhaps combine them to be able to cope with the current geopolitical developments.

The MCSC offers a forum for you, dear guests, to engage in such thinking and hence fostering the understanding and collaboration among your organizations and countries.

I wish us all a great conference. See you there.

Sincerely,

Claudia Eckert

Chairwoman of Security Network Munich
& Executive Director of Fraunhofer AISEC (Munich)

Security Network Munich

EDITORIAL

A Global Approach to Safer Technology

From Artificial Intelligence (AI) and extended reality to a broader adoption of cloud technology, the next generation of innovators and entrepreneurs have significant opportunities to succeed in the global technology ecosystem; but, these opportunities within the digital economy come at a price. The technology environment is rife with safety risks to each of us.

What is the responsibility of global governments and manufacturers to ensure we are building a secure ecosystem?

The current market incentivizes technology creators to prioritize speed and "first to market" over "secure to market," at the cost of product safety. Technology companies are often revered for their fast-paced and bold approach; but, in moving quickly, the safety of customers is often deprioritized, which is a condition we have come to expect and accept.

As technology innovation accelerates, we must demand that technology manufacturers adopt a practice and culture of secure innovation – where they intentionally design, develop, ship, and maintain safer technology from the beginning. Safe technology and products should be the default. We must demand that companies view technology product safety as a CEO-level strategic goal, not a niche area for technologists.

The Cost of Unsafe Technology

The current environment and business operating models unfairly place the burden of staying cyber safe on customers, who are often individuals and small and medium-sized businesses that don't have the resources or expertise to compensate for unsafe products.

When it comes to technology product safety, we have created a culture of "blaming the victim." We blame individuals for not enabling strong passwords and MFA, but never the manufacturer for making those actions optional and hard to enable. We blame the individual for not patching their system, but never the manufacturer that develops vulnerable software. We've normalized the creation of a market for security products that attempts to compensate for unsafe products, adding licensing and staffing costs to already stretched budgets. We witness a booming industry in incident response made possible by our reliance on unsafe code and products. Those costs are borne by customers when the burden of safety should be absorbed by the technology manufacturer.

This culture of unsafe technology also poses unacceptable risks to those who depend on it for living and livelihoods, including health care, finance, and K-12 education. When technology safety is not prioritized, the effects can be far-reaching and lead to devastating consequences, including school districts being shut down and food supply chains and the digital infrastructure upon which we rely for communication being disrupted.

Creating Safer Products

Technology product safety must be the standard. We can no longer accept that manufacturers introduce unsafe and flawed products into our digital economy and critical infrastructure and expect those costs to be absorbed by the users and third parties, rather than the manufacturers themselves. We are addressing only the symptoms of these vulnerabilities while unsafe development practices accelerate.

The Biden Administration is drawing greater attention to this issue through efforts to ensure supply chain security. We can begin to create a culture of secure innovation by ensuring greater transparency in supply chains through efforts such as adoption of Software Bill of Materials (SBOM). Additionally, the United States Government is working to use its power of procurement, as outlined in the Administration's 2021 Executive Order, to require industry to implement specific security practices in technology products sold to the federal government.

Senior executives and Boards must prioritize the creation of a culture of safety and security. At the Cybersecurity and Infrastructure Agency (CISA), we recently launched a Corporate Cyber Responsibility initiative. Our objective is to work with Boards and senior executives to prioritize cybersecurity and to offer best practices, such as those outlined in the Cyber Performance Goals (CPGs), which companies can follow to ensure they are making Board decisions that prioritize cyber security and cyber safety. We will work with industries and associations representing those industries to ensure cyber risk is identified as a corporate risk and is treated as such. Boards and senior executives must understand the cyber risk management profile of their companies and make business decisions aligned with that profile, accounting for downstream safety implications that a company's decisions may have on their customers.

A Global Solution

Prioritizing secure innovation, as well as safe and secure products, will require a global effort. We often talk about how cybersecurity does not recognize geographic boundaries – yet our policies for cybersecurity are constrained by geographic boundaries; they are created by a nation for a nation. We must instead invest in a global effort that mandates secure innovation and safe products, across all companies and industries, regardless of where their global headquarters reside.

As world leaders in cybersecurity, we must collaborate to demand technology manufacturers take ownership of the safety of their products, and thereby the cyber safety of their customers. We must change the global culture and ecosystem so that unsafe development tools and processes are no longer permitted and embrace an approach that assumes security, accountability, and responsibility.

Secure innovation is a unique opportunity for global cooperation, engagement, and action.

Kiersten E. Todt

Chief of Staff at the Cybersecurity and Infrastructure Security Agency (CISA)

Bob Lord

Senior Technical Advisor

MUNICH CYBER SECURITY CONFERENCE (MCSC) 2023

Cyber Security: Who is in Charge? – Dealing with Blurred Lines of Responsibility

THURSDAY, FEBRUARY 16TH

2:00–2:15 p.m.	**Welcome**	**Claudia Eckert** Chairwoman of Security Network Munich & Executive Director of Fraunhofer AISEC (Munich)
	Opening Keynote	**Judith Gerlach** Bavaria's State Minister of Digital Affairs (Munich)
2:15–2:35 p.m.	**Fireside Chat**	**Kemba Walden** Acting National Cyber Director in the Executive Office of the U.S. President (Washington D.C.) in conversation with **Christopher Krebs**, Founding Partner of the Krebs Stamos Group (Washington D.C.)
2:35–3:20 p.m.	**First Panel:** Cybersecurity - Who is in Charge? Managing Different Lines of Responsibility **Moderator: Ciaran Martin** Professor at University of Oxford and Former Director of the UK's National Cyber Security Centre (Oxford)	**Despina Spanou** Head of Cabinet for European Commission Vice President Margaritis Schinas (Brussels) **Andreas Könen** Director General for Cyber and Information Security at Federal Ministry of the Interior and Community (Berlin) **Kai Horten** Partner at AltoPartners Germany (Munich) **Robert Strayer** Executive Vice President of Policy at the Information Technology Industry Council (Washington D.C.)
3:20–3:40 p.m.	**Fireside Chat**	**Margaritis Schinas** Vice President of the EU Commission (Brussels) in conversation with **Ralf Wintergerst**, Group CEO at Giesecke+Devrient (Munich)
3:40–4:20 p.m.	**Coffee Break**	
4:20–4:35 p.m.	**Impulse**	**Sir Alex Younger** Former Chief of Secret Intelligence Service MI6 (London)
4:35–5:20 p.m.	**Second Panel:** Dual Use: Merging Defenses in Cyber – The Way Forward? **Moderator: Alexander Schellong** Vice President Cybersecurity at Schwarz Group (Munich)	**Mieke Eoyang** Deputy Assistant Secretary of Defense for Cyber Policy at U.S. Department of Defense (Washington D.C.) **Sandra Joyce** Vice President at Mandiant Intelligence (Washington D.C.) **Alix Carmona** Vice President and Head of Cyber Programmes at Airbus Defence and Space (Munich) **Robert Koch** General Staff Officer of the Federal Armed Forces (Munich)

5:20–5:50 p.m.	**Spot-on:** Looking beyond - Other Dimensions of Cyber **Moderator: Gregor P. Schmitz** Editor-in-chief at Stern Magazine (Hamburg)	**Sabine von der Recke** Member of the Management Board at OHB System AG (Bremen) **Philip Venables** Vice President and Chief Information Security Officer, Google Cloud (Mountain View) **Christopher Ahlberg** CEO of Recorded Future (Washington D.C.)
5:50–6:30 p.m.	**Coffee Break**	
6:30–6:40 p.m.	**World View**	**Akihiro Wada** Chair of Working Group at Committee on Cyber Security, Keidanren (Tokyo)
6:40–7:30 p.m.	**Third Panel:** Name of the Game: Teamplay – Overcoming Cyber Gaps **Moderator: Geoff Brown** Vice President at Recorded Future and Former CISO New York City (New York)	**Erkki Leego** Director of EU CyberNet at the Estonian Information System Authority (Tallinn) **Thomas Boué** Director General for Policy at BSA | The Software Alliance (Brussels) **Thomas Rosteck** Division President Connected Secure Systems at Infineon (Munich) **Jessica Keiser** Vice President Cyber Defense Center at Bayer AG (Leverkusen)
7:30 p.m.	**Greeting**	**Roland Weigert** Bavaria's State Vice Minister of Economic Affairs (Munich)
7:35 p.m.	**Reception Party**	

FRIDAY, FEBRUARY 17TH

9:00–9:15 a.m.	**Keynote** **Moderator: Oliver Rolofs** Founder and Managing Partner of COMMVISORY (Munich)	**Catherine de Bolle** Executive Director of Europol (The Hague)
9:15–10:00 a.m.	**Fourth Panel:** Talking about Resilience **Moderator: Jannis Brühl** Head of Tech Reporting at Süddeutsche Zeitung (Munich)	**David Wolpoff** Chief Technology Officer of Randori (Denver) **Mikko Karikytö** Chief Product Security Officer & Head of Product Security at Ericsson (Helsinki) **Srdan Dzombeta** Partner at EY (Berlin) **Nicholas Leiserson** Assistant National Cyber Director for Cyber Policy & Programs (Washington D.C.)
10:00–10:10 a.m.	**Vantage Point:** Investment Security	**Paul Rosen** Assistant Secretary of the Treasury for Investment Security (Washington D.C.)
10:10–10:55 a.m.	**Talking Heads:** Cybercrime: Lines of Action **Moderator: Marc Raimondi** Chief of Staff at Silverado Policy Accelerator (Washington D.C.)	**John P. Carlin** Partner at Paul Weiss (Washington D.C.) **Bryan Smith** Section Chief for FBI's Cyber Criminal Operations Section (Washington D.C.) **Nicholas Warner** Advisor at SentinelOne (Boston) **Valerie M. Cofield** Chief Strategy Officer of the U.S. Cybersecurity and Infrastructure Security Agency (Washington D.C.)
10:55–11:05 a.m.	**Impulse**	**Robert Silvers** Under Secretary for Strategy, Policy and Plans at the U.S. Department of Homeland Security (Washington D.C.)
11:05–11:50 a.m.	**Fifth Panel:** Geopolitical Dynamics: Tectonic Shifts in Cyber **Moderator: David Lashway** Co-chair of Sidley Austin LLP (Washington D.C.)	**Dmitri Alperovitch** Executive Chairman of Silverado Policy Accelerator & Co-Founder of CrowdStrike (Washington D.C.) **Liesyl Franz** Acting Deputy Assistant Secretary at the U.S. Department of State's Bureau of Cyberspace and Digital Policy (Washington D.C.) **Michael Rogers** Former Commander of the U.S. Cyber Command and Director of National Security Agency (New York)
11:50 a.m.–12:20 p.m.	**Coffee Break**	

12:20–12:30 p.m.	**Vantage Point**	**Mauro Vignati** Advisor Digital Technologies of Warfare at the International Committee of the Red Cross (Geneva)
12:30–12:45 p.m.	**Guest of Honor** **Moderator: Stormy-Annika Mildner** Executive Director Aspen Institute Germany (Berlin)	**Kaja Kallas** Prime Minister of Estonia (Tallinn)
12:45–1:00 p.m.	**Closing Keynote** **Moderator: John Carlin** Partner at Paul Weiss (Washington D.C.)	**Lisa Monaco** Deputy Attorney General, U.S. Department of Justice (Washington D.C.)
1:00–1:30 p.m.	**Sixth Panel:** The Way Forward: Making Alliances Work **Moderator: Jeff Greene** Senior Director for Cybersecurity Programs at the Aspen Institute (Washington D.C.)	**Vivian Schiller** Executive Director at The Aspen Institute (Washington D.C.) **Ciaran Martin** Professor at the University of Oxford and Former Director of the UK's National Cyber Security Centre (Oxford) **Claudia Gherman** Senior Policy Manager for Digital Resilience at Digital Europe (Brussels)
1:30 p.m.	**End**	

INSTITUTIONAL PARTNERS:

MEDIA PARTNERS:

DISTINGUISHED GUEST OF HONOR

Kaja Kallas

Prime Minister of Estonia (Tallinn)

Kaja Kallas has been Prime Minister of Estonia since January 2021. She has been the leader of the Reform Party since 2018, and a Member of Parliament from 2019 to 2021, and previously from 2011 to 2014. Between the two terms at the Estonian Parliament, from 2014 to 2018, Kallas served as a Member of the European Parliament (representing the Alliance of Liberals and Democrats for Europe), where her primary focus was on the Digital Single Market strategy, and energy and consumer policies. Before entering politics, she was an attorney-at-law, specialising in European and Estonian competition law, and a partner in two law firms. Prime Minister Kallas has been awarded the CEPA Transatlantic Leadership Award, the 2022 Grotius prize, the Hayek International Prize, and the European Prize for Political Culture. She is married and the mother of two sons and a daughter.

CONFERENCE MODERATOR

Kai Hermsen

twinds Foundation (Brussels)

Kai Hermsen is a “trust in tech” activist. He believes all people need to understand current digital topics and how they impact their lives, to enable trust in technology and good stewardship of our societies. He is currently building the "twinds foundation" concerned with establishing open-source "disposable identities" as a key technical enabler for building trust online. In addition, he advises and coaches different organizations on matters of digital trust and cybersecurity. With charitable organization "Identity Valley" and all it´s partners, he actively drove the transition towards a more responsible digital space along the "Digital Responsibility Goals". At “Siemens”, he demonstrated in practice how to transform and build trust through leading the "Charter of Trust", a global initiative of 17 corporations collaborating to strengthen security of the digital space. As a father of two, he is passionate about finding balance in life to enable the best work and most rewarding personal lives.

SPEAKERS

Claudia Eckert

Chairwoman of Security Network Munich & Executive Director of Fraunhofer AISEC (Munich)

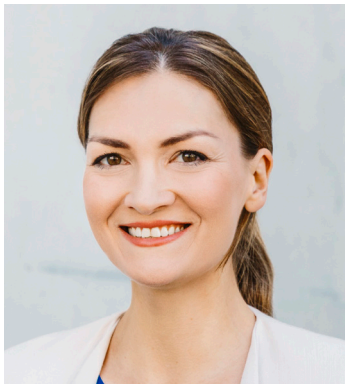
Prof. Dr. Claudia Eckert is executive director of the Fraunhofer Institute for Applied and Integrated Security AISEC in Garching and professor at the Technical University of Munich, where she holds the Chair for IT Security in the department of Informatics. Her research interests include the development 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. The results of her research have been published in over 160 peer-reviewed technical papers. Since January 1st, 2018, she has been the spokesperson for the Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT, which bundles the expertise of more than 20 Fraunhofer institutes to develop and implement new cognitive solutions from sensors to edge devices to cloud platforms for digitization, especially in industrial environments. 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. In expert committees, she is involved in shaping the technical and scientific framework conditions in Germany and in the design of scientific funding programs at the EU level.

Kemba Walden

Acting National Cyber Director in the Executive Office of the U.S. President (Washington D.C.)

Kemba Eneas Walden is the Acting National Cyber Director in the Office of the National Cyber Director. Kemba served as the inaugural Principal Deputy National Cyber for 8 months where she co-led the organization, overseeing the development and growth of the office. During her tenure, the Office of the National Cyber Director drafted the National Cybersecurity Strategy, managed implementation of Executive Order 14028, and spearheaded the first ever National Cyber Workforce and Education Strategy. Previously, she served as Assistant General Counsel in Microsoft's Digital Crimes Unit (DCU) responsible for launching and leading DCU's Ransomware Program. Kemba also served as a working group co-chair of the Ransomware Task Force and contributed to its report. Kemba started her career at Microsoft as Senior Counsel for Cyber and Democracy providing legal counsel to the Defending Democracy Program through the 2020 Presidential Election. Prior to Microsoft, Kemba spent a decade in government service at the Department of Homeland Security. At DHS, Kemba held several attorney roles, specifically as the lead attorney for the DHS representative to the Committee on Foreign Investment in the United States (CFIUS) and then as a cybersecurity attorney for the newly created Cybersecurity and Infrastructure Security Agency (CISA), and its predecessor, which is responsible for cybersecurity, telecommunications, and infrastructure resilience. Kemba negotiated complex data protection, information sharing, risk mitigation, and national security agreements, supported DHS's cybersecurity and risk management efforts in several critical infrastructure sectors. Upon her departure from DHS, her energy was spent as the primary cybersecurity legal advisor to the Elections Task Force (now known as the Elections Security Initiative). In addition to her work at Microsoft, Kemba was appointed to the inaugural Cyber Safety Review Board and serves as an Adjunct Professor at Georgetown University in the School of Continuing Studies teaching a course entitled "Information Security Laws and Regulatory Policy." Kemba graduated from Hampton University in Hampton, Virginia with a B.A. in Political Science, from Princeton University's School of Public and International Affairs with a Master's in Public Affairs, and from Georgetown University Law Center.

SPEAKERS



Judith Gerlach

Bavaria's State Minister of Digital Affairs (Munich)

Judith Gerlach is Bavaria's State Minister of Digital Affairs. She has headed the ministry since its foundation in November 2018. As the first digital minister in Germany, Gerlach controls and oversees the expansion of digital services for citizens and businesses. The minister also represents Bavaria vis-à-vis the federal government, for example, through the IT planning council. Gerlach champions a technologically open digital policy, which secures the interests of every citizen at its core. As the youngest member of the cabinet at only 37, the Minister of State fights for the interests of the younger generation. She was included in the "Top 40 under 40" by Germany's leading business magazine Capital.

Christopher C. Krebs

Founding Partner of the Krebs Stamos Group (Washington D.C.)

Christopher Krebs is Founding Partner of the Krebs Stamos Group and Chair of the Commission on Information Disorder at the Aspen Institute. He previously served as the first director of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) where he oversaw the Agency's efforts to manage risk to the nation's businesses and government agencies, bringing together partners to collectively defend against cyber and physical threats. Before serving as CISA Director, Mr. Krebs was appointed in August 2017 as the Assistant Secretary for Infrastructure Protection. Mr. Krebs joined the DHS in March 2017, first serving as Senior Counselor to the Secretary. Prior to coming to DHS, he led Microsoft's U.S. cybersecurity policy efforts. Mr. Krebs holds a bachelor's degree in environmental sciences from the University of Virginia and a J.D. from the Antonin Scalia Law School at George Mason University.

Despina Spanou

Head of Cabinet of the Vice President of the European Commission Margaritis Schinas (Brussels)

Despina Spanou is the Head of the Cabinet of the Vice President of the European Commission overseeing the European Union's policies on security, migration and asylum, health, skills, education, culture and sports. Her work on security consists in coordinating all areas under the heading of the EU Security Union, ranging from counter-terrorism, organised crime and cyber-security to hybrid threats. Previously, she was Director for Digital Society, Trust and Cybersecurity at the Directorate-General for Communications Network, Content and Technology (DG CONNECT) of the European Commission. In this capacity, Ms Spanou was responsible for the European Union's cybersecurity policy and law. Ms Spanou has 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, bodies and agencies (CERT-EU). She is a founding member of the Women4Cyber initiative and advocate for the need for more cybersecurity experts in Europe. Despina Spanou is a member of the Athens Bar Association and holds a Ph.D. in European law from the University of Cambridge.

SPEAKERS

Andreas Könen

Director General for Cyber and Information Security at Federal Ministry of the Interior and Community (Berlin)

Andreas Könen is the Director General CI Cyber and Information security. Previously he was the Head of Directorate IT II IT and cyber security; secure information technology and ÖS III Cyber security in the field of law enforcement and domestic intelligence by the German Federal Ministry of the interior. Before it he was the Vice President of the German "Federal Office for Information Security (BSI)". Mr Könen, a graduate mathematician, joined the BSI in 2006, taking on the post as the head of the executive staff of the BSI Director General. In 2009 he became the head of the division "Security in Applications and Critical Infrastructures" and subsequently head of the department "Security Consulting and Coordination". Prior to BSI, Mr Könen held various positions in the field of information technology within the German Federal Administration, including executive functions.

Kai Horten

Partner at AltoPartners Germany (Munich)

Kai Horten is a Managing Partner at AltoPartners I Jack Russell Consulting. AltoPartners is a Global Alliance of owner-managed HR consultancies, focusing on Leadership Advisory and Executive Search. Within this Alliance, Kai heads the Aerospace & Defence Practice. Before joining AltoPartners I Jack Russell Consulting in 2020, he was CEO of ESG Elektroniksystem- und Logistik GmbH, a trusted supplier to the German MoD as well as to major automotive OEMs in the domain of system integration and support, including cyber security aspects. Prior to that, he was CEO of Premium AEROTEC as well as MD of Atlas Elektronik, major players in the European Aerospace and Defence landscape. Prior to 2005, he held several management positions in today's Airbus Defence and Space and Airbus Helicopters. Kai Horten holds a master's degree (Dipl.-Ing. Univ) in aerospace engineering from the German Armed Force University in Munich.

Robert Strayer

Executive Vice President of Policy at the Information Technology Industry Council (Washington D.C.)

Rob Strayer is the Executive Vice President for Global Policy at the Information Technology Industry Council (ITI). He leads the technology sector's efforts to shape pro-innovation policy in major global markets on a wide range of issues, including cybersecurity, privacy, data flows, and artificial intelligence. Prior to joining ITI, Strayer served as the Deputy Assistant Secretary of State for Cyber and International Communications Policy at the U.S. State Department. In that role, he led dozens of dialogues with foreign governments on technology regulation and cybersecurity policy issues, including the importance of reliance on communications infrastructure from trusted vendors. He was named as an ambassador by the President to lead the 90-plus person U.S. delegation to the International Telecommunication Union (ITU) Plenipotentiary Conference in 2018. Before working at the State Department, Strayer was the general counsel for the U.S. Senate Foreign Relations Committee, and previously practiced telecommunications law at WilmerHale.

SPEAKERS

Margaritis Schinas

Vice President of the EU Commission (Brussels)

Margaritis Schinas took office as Vice President of the European Commission under President Ursula Von Der Leyen in December 2019. He is entrusted with the portfolio for Promoting our European Way of Life. In this capacity, he oversees the EU's policies for Security Union, migration, skills, education and integration. As Vice President in charge of the Security Union, he oversees and coordinates all strands of the European Commission's work under the Security Union, including tackling terrorism and radicalisation, disrupting organised crime, fighting cybercrime, stepping up cybersecurity, protecting critical infrastructures or addressing hybrid threats. Mr Schinas has also served as a Member of the European Parliament. Upon the completion of his parliamentary term of office, he returned to the European Commission and held various senior positions. In particular, in 2010, President Barroso appointed Mr Schinas as Deputy Head of the Bureau of European Policy Advisers. Later he served as Resident Director and Head of the Athens Office of the European Commission's Directorate-General for Economic and Financial Affairs (DG ECFIN). In 2014, President Juncker appointed Mr Schinas as the Chief European Commission Spokesperson. Mr Schinas has been working for the European Commission in various positions of responsibility since 1990. Margaritis Schinas holds an MSc on Public Administration and Public Policy from the London School of Economics, a Diploma of Advanced European Studies on European Administrative Studies from the College of Europe in Bruges and a Degree in Law from the Aristotelean University of Thessaloniki.

Ralf Wintergerst

Group CEO at Giesecke+Devrient (Munich)

Dr. Ralf Wintergerst is Chairman of the Management Board of Giesecke+Devrient (G+D). Alongside his duties as Group CEO, he is responsible for the Central Services departments of Information Systems, Corporate Security, Compliance Management and Auditing, Corporate Communications, Mergers & Acquisitions, Corporate Strategy, Corporate Development, Legal Services, and Corporate Governance. In addition, he holds various positions related to IT security issues, including as Chairman of the Advisory Board of the Alliance for Cyber Security, which was established by the German Federal Office for Information Security (BSI) and has become the country's largest cyber security initiative.

Sir Alex Younger

Former Chief of Secret Intelligence Service MI6 (London)

Sir Alex Younger is the Former Chief ("C") of the Secret Intelligence Service, also known as MI6. He served in this role for six years, from 2014-2020 and in 2019 became the longest-serving MI6 Chief in 50 years. Sir Alex Younger joined MI6 in 1991. He was posted to Europe and the Middle East, and Afghanistan. He spent most of his career as an operational case officer. In 2009, Sir Alex Younger became the head of counter-terrorism, during which he was involved in security for the London Olympics 2012. Alex became the UK's Spy Chief, a position known as "C" in 2014. During this period he focussed on the transformation of his service, aimed at making technology more of an advantage to MI6 than it was to their adversaries. He also maintained a network of intelligence chiefs worldwide, covering the spectrum from allies to adversaries. He advised the Prime Minister on intelligence and security matters, including as a member of the National Security Council. Prior to joining MI6, he read economics, as well as computer science, at St. Andrew's University and was an infantry officer in the British Army (Scots Guards).

SPEAKERS

Mieke Eoyang

Deputy Assistant Secretary of Defense for Cyber Policy at U.S. Department of Defense (Washington D.C.)

Ms. Mieke Eoyang is the Deputy Assistant Secretary of Defense for Cyber Policy. The Cyber Policy office is responsible for establishing DoD cyberspace policy and strategy, providing guidance and oversight on DoD cyberspace activities, and managing DoD's primary external relationships across the U.S. government, key domestic stakeholders, and our allies and partners. Prior to that she was the Senior Vice President for the National Security Program at the think tank, Third Way, where she led their work on a wide range of national security issues including on foreign policy, Congress' role in the national security policymaking process, non-proliferation, intelligence oversight, electronic surveillance, cybersecurity. She was the founder of the organization's Cyber Enforcement Initiative which focused on improving the government's efforts to impose consequences on the human behind malicious cyber activity. Before joining Third Way, she was the Chief of Staff to Rep. Anna G. Eshoo (D-CA) having previously served as the Subcommittee Staff Director for Intelligence Community Management on the House Permanent Select Committee on Intelligence. While there, she was the committee's lead for cybersecurity, personnel management and worked on electronic surveillance reform, among other issues. Prior to that, she served as the Defense Policy Advisor to Senator Edward M. Kennedy, advising him on all matters related to the Senate Armed Services Committee and Defense Appropriations during the Iraq War. Earlier in her career, she served as the lead Democratic Professional Staff Member on the House Armed Services Committee for the Military Personnel Subcommittee. Ms. Eoyang received her Juris Doctor from the University of California, Hastings College of the Law, and her Bachelor's Degree from Wellesley College.

Alexander Schellong

Vice President Cybersecurity at Schwarz Group (Munich)

Dr. Alexander Schellong heads the new Cybersecurity business and education activities of Schwarz Group, Europe's largest retailer and fourth largest retailer in the world. This includes working closely with XM Cyber, a leading Cybersecurity firm from Israel acquired by Schwarz Group in 2021 and leveraging Schwarz Group's sovereign Cloud offering STACKIT. He has 20 years of experience working for CSC (DX.C, GDIT), Capgemini, Algeco Group, Rohde & Schwarz Cybersecurity and INFODAS. Alexander has extensive experience in strategic consulting, general management, business unit leadership and mission critical international project and operations management in Europe, Middle East, Africa and Asia for the U.S. government, German government, European Commission, and other commercial clients. His domain expertise covers among others eGovernment, Cybersecurity, Cross Domain Solutions, Cloud, BPO, eCommerce or digital transformation. He has authored one book on CRM in the public sector and over 60 articles on a variety of topics at the intersection of technology, society, and organizations. In 2019, Alexander founded the non-profit initiative CYBERWOMEN to support networking among and growth of female information security experts from student to CxO across Germany. He studied and taught at Goethe-University Frankfurt am Main, Harvard Kennedy School, The University of Tokyo, Brandt School of Public Policy, Zeppelin University, Salzburg Management Business School, and Stanford University.

SPEAKERS

Sandra Joyce

Vice President at Mandiant Intelligence (Washington D.C.)

Sandra Joyce is a cybersecurity leader and has been head of Mandiant Intelligence since 2017. She oversees threat research activities and operations of the Mandiant Intelligence organization and joined Google in 2022, following Google's acquisition of Mandiant. Sandra is an officer in the U.S. Air Force Reserve, serving as a faculty member at the National Intelligence University. She is also a member of the Aspen Institute Cybersecurity Working Group, sits on the strategic council of the Silverado Policy Accelerator, and is a member of the Institute for Security and Technology's Ransomware Task Force Steering Committee. She is regularly featured in international print and broadcast media to include CNN, NBC, Bloomberg, BBC World, Today Show, NPR, Wall Street Journal, Deutsche Welle, and others. 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 with her family.

Alix Carmona

Vice President and Head of Cyber Programmes at Airbus Defence and Space (Munich)

Alix Carmona is the Vice President and Head of the Airbus Defence and Space Cyber Programmes since 2021. With over 450 employees all over Europe, the cyber business of Airbus Defence and Space delivers high-level security solutions to governments, armed forces and institutions. Having protected Airbus Defence and Space's complex systems and networks for over 30 years, the mission of the business is to design, develop, integrate and deploy tailored reliable cyber security solutions, helping customers and partners who are facing similar challenges. Prior to that, Alix held several management positions in the Airbus Group and Airbus Defence and Space, mainly in Finance and Controlling for major programmes. Alix is French and German, and has been living in Munich for the last 16 years. She speaks French, German and English fluently. Alix holds a Master of Science in Management from HEC Paris Business School.

Sabine von der Recke

Member of the Management Board at OHB System AG (Bremen)

Sabine von der Recke is responsible for Political Relations, Customer Relations and Communications on OHB System AG's Management Board. Prior to this, she had been the Board Representative for Political and Government Affairs at OHB SE, the Group's holding company, since 2014. OHB SE is Germany's first listed space and technology company, employing around 3,000 people. She has also been the spokesperson for the German Offshore Spaceport Alliance (GOSA) since 2020. After studying political science at Philipps University in Marburg, she worked as a director of the Parliamentary office of serveral MoPs in the German Bundestag from 2008-2014, including being an advisor to the aviation and space group in the German parliament. Sabine von der Recke is a member of the DLR Senate, Vice President of the ZARM Sponsors' Association and a member of the Board of the Forum Luft- und Raumfahrt.

SPEAKERS

Robert Koch

General Staff Officer of the Federal Armed Forces (Munich)

Commander PD Dr. rer. nat. Dr. habil. Robert Koch is a General Staff Officer of the Federal Armed Forces. He joined the Navy in 1998 and studied computer science at the Universität der Bundeswehr. After operational and technical training, he served as Deputy- and then as Weapon Engineering Officer onboard of German frigates. After completing the National General/Admiral Staff Officer Course at the Bundeswehr Command and Staff College, Robert had assignments as Action Officer Cyber at the Bundeswehr Communication and Information Systems Command, as Head of Department Penetration Testing at the Bundeswehr Cyber-Security Center, and as Desk Officer Cyber Policy at the Federal Ministry of Defense. Currently, Robert is Section Head Interoperability and Verification, and Director of NATO Coalition Warrior Interoperability exploration, experimentation, examination, and exercise (CWIX) at NATO Allied Command Transformation. Robert holds a Diploma in Computer Science and a master's in military leadership and International Security; he received his PhD in 2011, his habilitation in 2017 and his Venia Legendi in 2018. He is a lecturer in Computer Science with course offerings ranging from introductory Cybersecurity for non-technical audiences to deep technical topics. His research focuses on attack vectors, attack and tamper detection, anonymity in cyberspace, and conducting and optimizing security analysis..

Gregor P. Schmitz

Editor-in-chief at Stern Magazine (Hamburg)

Gregor is editor-in-chief of STERN magazine, one of the largest and most iconic German (and global) magazine brands. Prior to that, he served as editor-in-chief of one of the leading German dailies and as a foreign correspondent for DER SPIEGEL, Germany´s newsmagazine, in Brussels and (from 2007 to 2013) Washington. During his time in DC, he covered the Obama White House and two presidential campaigns. Gregor was part of SPIEGEL's WikiLeaks and NSA coverage and was awarded the prestigious Arthur F. Burns, Henri Nannen Prize and Theodor Wolff-Prize for his reporting. His bestselling first book, co-authored with legendary investor and activist George Soros ("The tragedy of the European Union – Disintegration or Revival") was published by Random House and translated into more than ten languages worldwide. Before starting his work with SPIEGEL, Gregor headed the Brussels Office of Bertelsmann Foundation, one of Europe's largest think tanks. He is a graduate of Harvard University (MPA) and Cambridge University (MPhil) and holds a law degree from Munich University. He also studied at Sciences-Po Paris and earned a doctorate in political science. In addition to his writing, Gregor is a frequent radio and TV commentator in national and international programs. He is also a member of the Atlantic Council, a Young Leader of the American Council on Germany, a McCloy Scholar of the German National Merit Foundation and head of the Harvard Alumni association Germany. He was named "Editor-in- Chief 2020" and a "Journalist of the Year" by Germany's leading media publication Medium Magazin three years in a row.

SPEAKERS

Philip Venables

Vice President and Chief Information Security Officer, Google Cloud (Mountain View)

Phil Venables is VP and Chief Information Security Officer of Google Cloud. He is a computer scientist, software engineer, and expert in technology, security, and enterprise risk who has co-founded and led multiple corporate and industry-wide cybersecurity initiatives focused on safeguarding critical infrastructure in the financial sector. Previously, he served as Chief Information Security Officer and Chief Operational Risk Officer at Goldman Sachs for 20 years and was a Board Director at Goldman Sachs Bank. He co-founded and directed many of the U.S. Financial Services Sector critical infrastructure protection initiatives such as the FS-ISAC, FS-ARC and Sheltered Harbor. He is a member of President Biden's Council of Advisors on Science and Technology (PCAST).

Christopher Ahlberg

CEO of Recorded Future (Washington D.C.)

Dr. Christopher Ahlberg is the CEO of Recorded Future, the world's largest intelligence company, and Chairman of Hult International Business School. He is a member of the Royal Swedish Academy of Engineering Sciences.

Akihiro Wada

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

Mr Wada has assumed the chairpersonship of the Working Group on Cyber-Security Enhancement, Committee on Cyber Security, Keidanren since April 2022. At All Nippon Airways Co., Ltd., Mr Wada is Senior Director responsible for information security & IT architecture strategy (Digital Transformation Department). Through his career, he retains large-scale project management skills including overseas vendors as well as practical knowledge on the ISMS (Information Security Management System), the PCIDSS (Payment Card Industry Data Security Standard), and the Personal Information Protection Law. Mr Wada's public activities outside Keidanren and ANA include postings at the National Information Security Centre (NISC), the Ministry of Economy, Trade and Industry (METI), the Ministry of Land, Infrastructure, Transport and Tourism (MLIT), and the Cyber Risk Intelligence Centre – Cross Sectors Forum, where he is currently vice chair. Mr Wada holds a BSc (Science) from Kyushu University.

SPEAKERS

Erkki Leego

Director of EU CyberNet at the Estonian Information System Authority (Tallinn)

Erkki Leego is the Director of EU CyberNet at the Estonian Information System Authority. Erkki has more than 25 years of experience in IT management, cybersecurity, knowledge management and teaching. He has managed the digital transformation of the Estonian Parliament, the largest health care provider in Estonia – Tartu University Hospital, the Estonian Genome Center, and the University of Tartu. In the consulting company Leego Hansson, he has advised the IT management, digital transformation, and cybersecurity of more than 150 organizations with his team. Erkki has a master's degree in informatics from the University of Tartu and teaches IT strategic management in a master's course at the same university.

Geoff Brown

Vice President at Recorded Future and Former CISO New York City (New York)

Geoff Brown joined Recorded Future in January 2022 to accelerate the company's impact for the missions of global governments. Geoff built the centralized cybersecurity program for the City of New York as NYC's CISO and the founding Head of NYC Cyber Command (between 2016 and December 2021), and has prior experience in financial services and the U.S. Federal Government, including with the 9/11 Commission. Geoff is a member of Aspen Institute's Cybersecurity Group, a graduate of Middlebury College, and teaches intelligence and cybersecurity at the Nonproliferation and Terrorism Studies Department at the Middlebury Institute for International Studies in Monterey, CA.

Thomas Boué

Director General for Policy at BSA | The Software Alliance (Brussels)

Thomas Boué oversees the BSA | The Software Alliance's public policy activities in the Europe, Middle East and Africa region. He advises BSA members on public policy and legal developments and advocates the views of the ICT sector with both European and national policy makers. He leads on security and privacy issues as well as broader efforts to improve levels of intellectual property protection and to promote open markets, fair competition, and technology innovation in new areas such as cloud computing. Prior to joining BSA, Boué served as a consultant in Weber Shandwick where he advised clients on a wide range of technology and ICT-related policy issues and represented them before the EU institutions and industry coalitions. In this role, he also served as policy and regulatory adviser for both EU and US telecom operators. Prior to that Boué worked for the EU office of the Paris Chamber of Commerce and Industry where he was responsible for the lobbying activities towards the EU Institutions in the areas of trade, education, and labor, as well as for the organization and running of seminars on EU affairs for SMEs and business professionals. Boué holds a Master of Business Administration from the Europa-Insitut (Saarbrücken, Germany), a Certificate of Integrated Legal Studies (trilateral and trilingual Master's degree in French, English, German and European Law, from the Universities of Warwick (UK), Saarland (Germany) and Lille II (France) as well as a Bachelor of Arts in Law from the University of Lille II, France. He is based in BSA's Brussels office.

SPEAKERS

Thomas Rosteck

Division President Connected Secure Systems at Infineon (Munich)

Thomas Rosteck has been Division President Connected Secure Systems at Infineon Technologies AG since 2017. Thomas was born in 1966 in Offenbach am Main, Germany. He studied Business Administration and Computer Science at the Technical University of Darmstadt. He has been with Infineon since 1998 (Siemens AG until 1999).

Jessica Keiser

Vice President Cyber Defense Center at Bayer AG (Leverkusen)

Jessica Keiser has been Vice President Cyber Defense Center at Bayer AG since 2021. She and her department are responsible for cyber security and the identification and defense against cyber threats. She also represents the company in various external bodies, including the DCSO (Deutsche Cyber Sicherheitsorganisation GmbH). Her career started at a large German consumer goods company, where she held several global roles in Belgium, Germany and China in both IT and purchasing. Since 2017, her focus has been on cyber security, with the founding of a cyber defense organization and a cyber security awareness program. Jessica Keiser holds a Master's degree in Applied Economics and a Master after Master in Information Technology.

Roland Weigert

Bavaria's State Vice Minister of Economic Affairs (Munich)

Roland Weigert was born in 1968 and grew up in Hohenried in the district of Neuburg-Schrobenhausen in Upper Bavaria. After passing his A levels and finishing his training as a wholesale and foreign trade merchant, he joined the Federal Armed Forces in 1990 as an officer. At the same time, Roland Weigert studied Business and Organizational Sciences at the University of the Federal Armed Forces in Munich and graduated with a diploma degree in Business Administration "Dipl.-Kaufmann (Univ.)". From 1999, he worked as economic officer in the district of Neuburg-Schrobenhausen and was elected in 2008 Administrative Head of District of Neuburg-Schrobenhausen. He held this position for more than 10 years and left this position after his election to the Bavarian State Parliament in 2018. In 2018, Roland Weigert became Vice Minister and member of the Bavarian State Government.

SPEAKERS

Catherine de Bolle

Executive Director of Europol (The Hague)

Before taking up her post as Europol's Executive Director in May 2018, Catherine De Bolle served as General Commissioner of the Belgian Federal Police from 2012. Prior to her appointment as Belgian Police Commissioner, Ms De Bolle was Chief of Police in Ninove. In January 2015, she has received the title of Public Manager of the year. From November 2015 until November 2018, she was a member of the Executive Committee of Interpol. Ms De Bolle studied law at Ghent University and then went on to graduate from the Royal Gendarmerie Academy in Belgium.

Oliver Rolofs

Founder and Managing Partner of COMMVISORY (Munich)

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 long-standing 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.

David Wolpoff

Chief Technology Officer of Randori (Denver)

David Wolpoff (Moose) is co-founder and CTO of Randori. David is a recognized expert in digital forensics, vulnerability research and embedded electronic design. Prior to founding Randori, David held executive positions at Kyrus Tech, a leading defense contractor, and ManTech where he oversaw teams conducting vulnerability research, forensics and offensive security efforts on-behalf of government and commercial clients. David holds a Bachelor of Science and Master of Science degrees in Electrical Engineering from the University of Colorado.

SPEAKERS

Jannis Brühl

Head of Tech Reporting at Süddeutsche Zeitung (Munich)

Jannis Brühl is head of tech reporting at Süddeutsche Zeitung, Germany's major daily. He has been covering surveillance, cybersecurity, AI, platform regulation and tech policy for years, asking what technological changes mean for our politics, our economies, and society at large. Always keen to get a global view on things, he was an Arthur F. Burns Fellow at investigative nonprofit outlet Propublica in New York City, and was part of the international team of journalists investigating phone surveillance for the award-winning Pegasus Project.

Mikko Karikytö

Chief Product Security Officer & Head of Product Security at Ericsson (Helsinki)

Mikko Karikytö is the Chief Product Security Officer (CPSO) & Head of Product Security for Ericsson with accountability for security requirements, standards, strategy and architecture, related to product development and management, and overall accountability of product security and product privacy. He is senior advisor on Product and Solution Security to the CTO, and other executive Ericsson leaders. Mikko has previously worked as Head of Network Security and Head of PSIRT (Product Security Incident Response Team) responding, investigating and solving cyber security incidents and breaches with Ericsson customers globally. Mikko has also engaged in industry collaboration through organizations like ETIS, FIRST and EU Commission work groups. He has also provided Subject Matter Expertise for committee hearings of the UK parliament and the German Bundestag in 5G Security.

Srdan Dzombeta

Partner at EY (Berlin)

Dr. Srdan Dzombeta is a business graduate and Master of Laws (LL.M.). He studied at the Technical University Berlin, the University of California in Los Angeles and the Saarland University. He also holds a doctorate in Information Science and Technologies from Carlos III University in Madrid. Srdan Dzombeta is a partner and responsible for cybersecurity and data security. For more than 19 years he has been involved in the implementation of technical and organizational data security requirements for processes and procedures as well as in information technology. Srdan Dzombeta gained experience in the use of national and international legal norms and recognized standards particularly while working for several years with a leading international accounting firm. In particular, through his long-standig work on international projects, Srdan Dzombeta gained experience in the application of national and international laws and other legal standards and norms. Srdan Dzombeta has published a variety of academic papers and has published articles in national and international journals on information security and privacy issues. He is also a lecturer at various academies and universities. Srdan Dzombeta is member of the leadership team of EY Europe West and responsible for Cybersecurity & Privacy.

SPEAKERS

Nicholas Leiserson

Assistant National Cyber Director for Cyber Policy & Programs (Washington D.C.)

Nicholas Leiserson is the Assistant National Cyber Director for Cyber Policy and Programs. He previously served as the Office of the National Cyber Director's Deputy Chief of Staff. Prior to joining ONCD, Nicholas spent more than a decade on the staff of Congressman James R. Langevin, the principal author of the National Cyber Director Act, most recently as his Chief of Staff. A Connecticut native, Nicholas holds a degree in computer science from Brown University.

Paul M. Rosen

Assistant Secretary of the Treasury for Investment Security (Washington D.C.)

Paul Rosen serves as the Assistant Secretary of the Treasury for Investment Security. Appointed by the President and confirmed by the United States Senate on May 23, 2022, Mr. Rosen leads the Committee on Foreign Investment in the United States (CFIUS), the interagency committee established by Congress to review certain foreign investment into U.S. businesses for national security risks. Mr. Rosen advises the President and the Secretary of the Treasury about such risks including whether transactions should be cleared, blocked or otherwise mitigated to protect national security. The duties involve reviewing hundreds of transaction filings each year often amounting to hundreds of billions of dollars in merger and acquisition activity. Mr. Rosen has more than 15 years of experience in national and homeland security, investigations and law enforcement matters. Prior to joining Treasury, Mr. Rosen served as a partner at an international law firm where he led the national security practice and worked on cybersecurity, privacy, and government investigation matters. Before private practice, Mr. Rosen served for over a decade in senior government roles, including as Chief of Staff of the Department of Homeland Security during the Obama-Biden Administration, and in various roles at the Department of Justice including as a federal prosecutor in the Criminal Fraud Section of DOJ where he investigated and prosecuted financial crimes. For this work, Mr. Rosen was recognized by the Council of Inspectors General on Integrity and Efficiency (CIGIE) with the Investigative Award of Excellence. Mr. Rosen started his legal career as Counsel on the Senate Judiciary Committee after clerking for United States District Judge Gary Allen Feess (Ret.) in the Central District of California. Rosen received his J.D. from the University of Southern California where he graduated Order of the Coif, and his bachelor's degree, summa cum laude, from the University of Colorado.

Nicholas Warner

Advisor at SentinelOne (Boston)

An advisor with nearly 30 years in the IT and Cybersecurity field, Nicholas Warner leverages his years of experience to recommend transformative solutions that combat emerging risks facing enterprises today. He most recently played a key role in SentinelOne's growth over the past five years, and previously served as chief revenue officer (CRO), chief operating officer and president of security at the cybersecurity software company. Warner is particularly well known within the community of board members, and he has been a strong advocate for educating and preparing leaders on the latest cyber trends..

SPEAKERS

John P. Carlin

Partner at Paul Weiss (Washington D.C.)

John P. Carlin is co-head of Paul Weiss's Cybersecurity & Data Protection practice and a deeply accomplished litigator who advises industry-leading organizations on matters involving privacy and cybersecurity, crisis management, Committee on Foreign Investment in the United States (CFIUS), sanctions and export control, white collar defense and internal investigations. He has served as a top-level official in both Republican and Democratic administrations, including as the Acting Deputy Attorney General of the United States, as the top national security official for the U.S. Department of Justice, as the Chief of Staff of the FBI and as an experienced Assistant United States Attorney. Mr. Carlin has been featured or cited as a leading authority on cyber and economic espionage matters by numerous major media outlets, including The New York Times, The Washington Post, The Wall Street Journal, The Los Angeles Times, USA Today, CBS's 60 Minutes, NBC's Meet the Press, PBS's Newshour, ABC's Nightline and Good Morning America, NPR, CNN and Vanity Fair, among others.

Marc Raimondi

Chief of Staff at Silverado Policy Accelerator (Washington D.C.)

Marc Raimondi is the founder of the government relations and strategic communications consulting firm LexStrat, LLC, supporting corporate, academic and non-profit clients in the national security, public safety, cyber and technology markets. From March 2014 through July 2021, Marc led the national security related external communications and corporate outreach efforts for the U.S. Department of Justice, including stints serving as the top Justice Department spokesperson. Marc was detailed from the Justice Department to the White House's National Security Council (NSC) from November 2016 until June 2018, where he served as Director of Strategic Communications and was the lead communications advisor to the Assistants to the President for Homeland Security, Counterterrorism and Cybersecurity during two presidential administrations. While at the NSC, Marc also supported the intelligence, counterterrorism, cyber and aviation security teams and directorates. Prior to joining the Justice Department, Marc served for several years in private industry as Director of Global Government Relations and Communications at L3Harris Corporation's (LHX) Washington Operations. Before moving to the private sector in 2007, Marc held senior communications positions at the Departments of Homeland Security and Defense and started his career as an infantryman in the U.S. Army. Marc has worked on international advocacy projects for both government and corporate entities throughout the world including Central America, the Middle East, Europe, and Asia.

Ciaran Martin

Professor at University of Oxford and Former Director of the UK's National Cyber Security Centre (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 on 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.

SPEAKERS

Bryan Smith

Section Chief for FBI's Cyber Criminal Operations Section (Washington D.C.)

Bryan Smith has been employed by the Federal Bureau of Investigation (FBI) as a Special Agent since 2002 and currently serves as section chief for the FBI's Cyber Criminal Operations Section where he is responsible for the FBI's investigations and operations against cyber criminal actors and threats. Prior to his current role, Mr. Smith served as the assistant special agent in charge of the Cleveland Field Office's Cyber/White Collar Branch, unit chief of the FBI's Money Laundering and Bank Fraud unit, and as the FBI's detailee to the U.S. Securities and Exchange Commission where he assisted both agencies in insider trading, market manipulation, and investment fraud matters. His experience crosses over financial crimes, cyber, and virtual currency and in 2014 he initiated the FBI's first unit focused on cryptocurrency. A proponent of public private partnerships he has initiated several private sector outreach efforts to better leverage the complementary knowledge of both. Prior to the FBI, Mr. Smith worked as a consultant for Accenture and Deloitte & Touche and is a graduate of Bradley University with a degree in accounting.

Valerie M. Cofield

Chief Strategy Officer of the U.S. Cybersecurity and Infrastructure Security Agency (Washington D.C.)

Valerie M. Cofield serves as the Chief Strategy Officer of the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Ms. Cofield serves as the principal policy and strategic adviser to CISA leadership and senior management, integrating strategy across all the organization's mission areas and ensuring policy, strategy, and operational consistency throughout the agency. Prior to CISA, Ms. Cofield served at the FBI for 22 years in a variety of roles. She was a Deputy Assistant Director (DAD) for the Cyber Capabilities Branch within the Federal Bureau of Investigation's (FBI) Cyber Division where she led coordination and deployment of the division's technical tools and capabilities, and oversaw cyber-related training, recruiting, hiring, and budgeting for the division. She also served in a senior executive role as chief of staff of the Science and Technology Branch and as a DAD of the Digital Transformation Office (DTO), where she engaged with interagency partners and other key stakeholders on policy issues related to current and emerging technologies and their impact on law enforcement. In 2019, Ms. Cofield was selected as the FBI's senior detail to the Cyberspace Solarium Commission. This Congressional Commission was authorized through the FY2019 National Defense Authorization Act (NDAA). Its mission was to develop a national strategy for preventing cyberattacks of significant consequences. While on the Commission, Ms. Cofield was a Senior Director and Task Force Lead. The Commission completed its report in March of 2020 with over 75 recommendations, 25 of which were included in the FY21 NDAA and enacted into law. Ms. Cofield holds a bachelor's degree in Economics with a minor in Accounting from UCLA.

SPEAKERS

Robert Silvers

Under Secretary for Strategy, Policy and Plans at the U.S. Department of Homeland Security (Washington D.C.)

Robert Silvers was confirmed by the Senate as the Under Secretary for Policy on August 5, 2021. He is responsible for driving policy and implementation plans across all of DHS's missions, including counterterrorism; cybersecurity, infrastructure security, and resilience; border security and immigration; international affairs; and trade and economic security. Mr. Silvers previously served in the Department of Homeland Security during the Obama-Biden Administration as Assistant Secretary for Cyber Policy. In that role he oversaw private sector engagement, federal government incident response, and diplomatic outreach pertaining to cybersecurity and emerging technology. Mr. Silvers also previously served as DHS's Deputy Chief of Staff, managing execution of policy and operational priorities across the entire Department. Prior to his appointment, Mr. Silvers was a partner at the law firm Paul Hastings LLP, where his practice focused on cybersecurity and data privacy, government security review of foreign investments, and investigations and litigation at the intersection of law and national security. After graduating law school, he clerked for Judge Kim McLane Wardlaw of the U.S. Court of Appeals for the Ninth Circuit. Mr. Silvers holds a J.D. from New York University School of Law and a B.A. from the University of Pennsylvania. He taught as an adjunct professor in the M.S. in Cybersecurity Risk and Strategy Program co-offered by the NYU Law School and NYU Tandon School of Engineering. A New York City native, Mr. Silvers lives in Washington, D.C. with his wife and their two children.

Dmitri Alperovitch

Executive Chairman of Silverado Policy Accelerator & Co-Founder of CrowdStrike (Washington D.C.)

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. His writing on geopolitics, foreign policy and cybersecurity issues has appeared in major news outlets including the New York Times, the Washington Post, and Foreign Affairs, and he is a regular contributor to national broadcast news programs including PBS Newshour and NBC News. Alperovitch is also an active angel investor and board member of multiple high-growth technology companies. He has been named as one of Fortune Magazine's "40 Under 40" most influential young people in business and Politico Magazine has featured Alperovitch as one of "Politico 50" influential thinkers, doers and visionaries transforming American politics. In 2013, Alperovitch received the prestigious recognition of being selected as MIT Technology Review's "Young Innovators under 35" (TR35) and Foreign Policy's Leading Global Thinkers, and he was named a "D.C. Tech Titan" and one of the 500 most influential people in Washington by Washingtonian Magazine in 2022. In 2021, he launched the Alperovitch Institute for Cybersecurity Studies at Johns Hopkins University's School of Advanced International Studies (SAIS). He is the host and creator of Silverado's popular "Geopolitics Decanted" podcast, dedicated to expert analysis of the war in Ukraine as well as broader issues related to industrial policy, semiconductors, cybersecurity and economic and ecological security.

SPEAKERS

Liesyl Franz

Acting Deputy Assistant Secretary at the U.S. Department of State's Bureau of Cyberspace and Digital Policy (Washington D.C.)

Liesyl Franz is the Acting Deputy Assistant Secretary for International Cyberspace Security in the U.S. Department of State's Bureau of Cyberspace and Digital Policy. She coordinates cyber policy issues across a broad range of issues that affect international cyberspace security and oversees the unit's three offices covering Global Policy, Plans, and Negotiations; International Engagement and Capacity Building; and Threat Management and Coordination. She was previously the director for the Office of International Engagement and Capacity Building and the Deputy Coordinator for the Bureau's predecessor Office of the Coordinator for Cyber Issues. Ms. Franz has over 20 years of cyber policy experience in the public and private sectors. In her 10-year tenure at the Department of State, she has served as delegation lead for multiple cyber engagements with bilateral and regional partners and multilateral negotiations including in the UN, the Internet Governance Forum (IGF), and the International Telecommunication Union (ITU), as well as regional venues such as the ASEAN Regional Forum (ARF) and the Organization of American States (OAS). Prior to her current position she led the office's cyber policy work in the Europe and Eurasian Region and on Internet governance policy, respectively. Previously, she served as Vice President for Cybersecurity and Global Public Policy at TechAmerica, an industry association representing global high technology companies; Director for Cybersecurity International Affairs and Public Policy in the U.S. Department of Homeland Security; and Director for Global Government Affairs at EDS Corporation. Ms. Franz holds a B.A. in Political Science from the University of Texas at Austin and an M.A. from the Elliott School of International Affairs at George Washington University.

David Lashway

Co-chair of Sidley Austin LLP (Washington D.C.)

David Lashway is co-chair of Sidley Austin LLP's highly ranked Global Privacy and Cybersecurity practice and a member of the firm's top ranked Crisis Management and Strategic Response team. He is acknowledged as one of the leading lawyers for crisis management, cybersecurity, data security incidents, misinformation, trade secret theft, and related investigation matters. He has advised private and public organizations on significant and 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 a number of Fortune 100 entities, and led the incident response, associated investigations and litigations for several companies impacted by the NotPetya malware incident. He routinely leads responses to ransomware-related matters. David has been regularly named as one of leading lawyers in surveys of the best lawyers for cybersecurity globally. In a recent ranking, The Legal 500 noted that clients describe him as "a brilliant lawyer and strategist. He is very intelligent and his performance in front of boards and management teams have been some of the best I have ever seen." Another client noted that "David Lashway is exceptionally knowledgeable and conversant in cyber incident response, cyber threat intelligence, legislation and authorities' issues, and national security matters." He is recognized as a leading lawyer in incident response in the 2022 edition of Chambers USA: America's Leading Lawyers in Business , receiving a Tier One ranking in Cyber Incident Response. He has been included on the list of leading Incident Response Lawyers since its inception, and is a sought-after speaker related to cybersecurity and national security matters. David has also served as lead counsel on matters for organizations facing difficult regulatory, legislative, and public policy issues across a range of industry sectors and subjects. David is fluent in multiple languages and regularly handles matters involving the global intelligence community and law enforcement.

SPEAKERS

Michael Rogers

Former Commander of the U.S. Cyber Command and Director of National Security Agency (New York)

Admiral Rogers is a member of the Board of Directors or Advisory Board to multiple companies in the private sector and works in the consulting and venture capital arenas across the globe while also speaking internationally to various business and academic groups in the areas of cyber, technology, leadership, crisis response and global security. He can be seen on major media outlets across the globe on occasion addressing those same issues. He is a Senior Fellow and Adjunct Professor with Northwestern University's Kellogg School of Management's Kellogg Executive Leadership Institute and works with DoD in the mentoring and professional development of its General and Flag officers. Mike served in the U.S. Navy for nearly 37 years culminating his service in uniform with a four year plus tour as both the Commander, U.S. Cyber Command and Director, National Security Agency. Admiral Rogers retired from the U.S. Navy in 2018 after nearly 37 years of naval service rising to the rank of four- star admiral. He culminated his career in uniform with a four plus year tour as the Commander of U.S. Cyber Command and Director, National Security Agency – creating the DoD's then newest combatant command and leading the largest intelligence organization in the free world. In those roles he worked with the leadership of the U.S. government, the DoD and the Intelligence community as well as their international counterparts in the conduct of cyber and intelligence activity across the globe. He also assisted in the development of national and international policy with respect to cyber, intelligence, privacy and technology – including extensive work with corporate leadership in the finance, IT, telecommunications and technology – and national security more broadly. Prior to his final duties he also served as Commander, U.S TENTH FLEET/Fleet Cyber Command and the Director of Intelligence for the Joint Chiefs of Staff and the Indo-Pacific Command. He is a graduate of Auburn University and holds a Masters in National Security (East Asia) and is a distinguished graduate of the National War College and a graduate of highest distinction from the Naval War College. He is also an MIT Seminar XXI Fellow and a Harvard Senior Executive in National Security alum.

Mauro Vignati

Advisor Digital Technologies of Warfare at the International Committee of the Red Cross (Geneva)

Mauro Vignati is adviser on new digital technologies of warfare at the International Committee of the Red Cross headquarters in Geneva, Switzerland. Mauro has 20 years of experience in cyber threat intelligence and cybersecurity. Before joining the ICRC, he worked for the Swiss federal police and the Swiss department of defence, where is set up several units dedicated to the cyber threat intelligence. He also worked for MELANI, Switzerland's first centre for public-private partnership on cybersecurity for critical infrastructure, and for the National Cyber Security Centre (NCSC.ch), where he was tasked to establish the Vulnerability Management Unit. He has a long experience in the prevention, identification, and analysis of advanced persistent threats, mainly coming from state-sponsored groups. He also spends his time researching in the field of digital technologies in different political and economic environments. He holds a master's degree in literature and an executive master's in criminology and he teaches at Universities in Berne, Geneva, and Lugano.

SPEAKERS

Lisa O. Monaco

Deputy Attorney General, U.S. Department of Justice (Washington D.C.)

Lisa O. Monaco is the 39th Deputy Attorney General of the United States. As the Deputy Attorney General, she is the Department's second-ranking official and is responsible for the overall supervision of the Department. The Deputy Attorney General serves as the Chief Operating Officer, and the Department's litigating and policy components, law enforcement agencies, and 93 U.S. Attorneys report to the Deputy. The Deputy Attorney General advises and assists the Attorney General in formulating and implementing the Department's policies and programs. A veteran of the Department of Justice, Deputy Attorney General Monaco served as a career federal prosecutor and in several leadership positions across the Department. She began her Justice Department career as Counsel to Attorney General Janet Reno and went on to serve as an Assistant United States Attorney (AUSA) for the District of Columbia, where she was a member of the Enron Task Force and received the Attorney General's Award for Exceptional Service, the Department's highest award. She thereafter served in several leadership roles: Chief of Staff at the Federal Bureau of Investigation to then Director Robert S. Mueller, III; Principal Associate Deputy Attorney General; and Assistant Attorney General for National Security, the first woman to hold that position. From 2013-2017, Deputy Attorney General Monaco was the Homeland Security and Counterterrorism Advisor to the President. In that role, she coordinated the Executive Branch's policy and response to a wide range of security issues – including the response to international and domestic terrorist incidents, cyber threats, and natural disasters – and advised the President on all aspects of counterterrorism policy and strategy. Deputy Attorney General Monaco has served in private practice and taught national security law. She was born and raised in Massachusetts and is a graduate of Harvard University and the University of Chicago Law School.

Stormy-Annika Mildner

Executive Director Aspen Institute Germany (Berlin)

In January 2021, Dr. Stormy-Annika Mildner (M.Sc.) became Director of the Aspen Institute Germany in Berlin, a renowned policy-oriented thinktank focusing on transatlantic relations and issues of global importance. As an adjunct professor, she teaches political economy at the Hertie School. From 2014 to 2020, she served as head of the department "External Economic Policy" at the Federation of German Industries (BDI), where she was responsible for international trade and investment issues. As Sherpa, she spearheaded the German Business7 Presidency (2015) and the German Business20 Presidency (2016-2017). Prior to joining BDI, she was Member of the Board of the German Institute for International and Security Affairs (SWP), worked as a lecturer at the John F. Kennedy Institute of the Free University of Berlin, and headed the program "Globalization and the World Economy" at the German Council on Foreign Relations (DGAP). She completed research fellowships at the American Institute for Contemporary German Studies and the Transatlantic Academy of the German Marshall Fund in Washington. She earned a Master of Science in international political economy from the London School of Economics and a PhD in economics from Freie Universität Berlin. During her doctoral studies, she conducted a one-year fellowship at the Yale Center for International and Area Studies (YCIAS) at Yale University.

SPEAKERS

Vivian Schiller

Executive Director at The Aspen Institute (Washington D.C.)

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.

Jeff Greene

Senior Director for Cybersecurity Programs at the Aspen Institute (Washington D.C.)

Jeff Greene is the Senior Director for Cybersecurity Programs at the Aspen Institute. Jeff joined Aspen in July of 2022 from the White House, where he served as the Chief for Cyber Response & Policy in the National Security Council's Cyber Directorate. Jeff led the NSC's defensive cyber and incident response efforts, and his team developed and drafted Executive Order 14028 (Improving the Nation's Cybersecurity). Jeff also ran the White House counter-ransomware effort and oversaw the whole-of-government effort to harden the cybersecurity of U.S. critical infrastructure in advance of Russia's further invasion of Ukraine. Jeff previously served as Director of the National Cybersecurity Center of Excellence at the National Institute of Standards and Technology (NIST). Prior to joining NIST he was the Vice President of Global Government Affairs and Policy at Symantec, where he led a global team of policy experts. While at Symantec Jeff also served as an appointed member of NIST's Information Security and Privacy Advisory Board and was a special government employee working on President Obama's 2016 Commission on Enhancing National Cybersecurity. Before Symantec Jeff worked on both the House and Senate Homeland Security Committees, was Counsel to the Senate's Special Investigation into Hurricane Katrina, and practiced law at a large Washington, D.C. firm.

Claudia Gherman

Senior Policy Manager for Digital Resilience at Digital Europe (Brussels)

Claudia joined DIGITALEUROPE in June 2021. She has a unique blend of policy expertise in digital and healthcare policy, combining work experience in-house, at Novartis, in trade associations, at the British Chamber of Commerce in Belgium and to the EU and MedTech Europe as well as in consultancy. Claudia is passionate about the digital transformation of our societies, including digital sustainability. A relentless learner, she is curious, analytical and good-humoured. Claudia holds an MA degree in International Relations (University of Bucharest/ École des hautes études en sciences sociales) and a BA degree in Political Science (University of Bucharest).

Steve Durbin

Chief Executive of Information Security Forum ISF

Steve Durbin is Chief Executive of Information Security Forum ISF. He is a frequent speaker on the Board's role in cybersecurity and technology.

Measuring Cybersecurity: The Importance of Quantifying Risks and Vulnerabilities

Cybersecurity measurement is a critical component of a successful cyber risk program. However, it can be challenging for both business leaders and security practitioners. Business leaders often struggle to comprehend information risk due to lack of cybersecurity knowledge, while security practitioners may get caught up in technical details, leading to confusion or misinformation.

To overcome these challenges, security practitioners should measure and report cybersecurity in a way that is easily understood by senior executives and leads to actionable outcomes. The following are the aspects that can be measured in cybersecurity:

- Controls: Measures put in place to counter threats and reduce information risk.
- Assets: Valuable items owned by the organization.
- Vulnerabilities: Weaknesses in the system that can be exploited by threats.
- Threat events: Actions initiated by threats that can cause harm to assets.
- Security incidents: Impacts to the business such as data breaches, downtime, system shutdown, etc.

These categories can be further broken down into numbers, time, or cost. For instance, numbers can measure the number of unpatched servers, the time it takes to identify an incident, or the cost of a security incident. Instead of focusing on metrics, security practitioners should concentrate on key performance indicators (KPIs) and key risk indicators (KRIs). KPIs and KRIs help answer questions related to information security risk, preparedness, and business priorities, such as regulatory compliance, cost of security incidents, and preparedness for attacks.

How Security Teams Can Measure Cybersecurity

Building the right measurement framework is a gradual, iterative process. Let's explore the five main steps involved in building a security measurement cycle:

1. Define Requirements: Engage with stakeholders to understand their needs and educate them on information risk. Ask probing questions and use bottom-up approach if necessary.

2. Select Key Indicators: Identify high-level indicators to support stakeholder requirements and consult all stakeholders. Focus on a few indicators that support decision-making.

3. Identify Metrics: Based on indicators, identify lower-level metrics from different categories of measurement.

4. Collect and Analyze Metrics: Begin collecting and analyzing data based on agreed-upon key indicators and metrics. Use accurate, timely, relevant, and trustworthy data. Automate collection process if possible.

5. Report Key Indicators: Report key indicators to decision-makers regularly and in a style agreed upon with stakeholders (e.g. dashboards or presentations). Review indicators after each cycle and revalidate with stakeholders.

After each reporting cycle, key indicators should be reviewed and revalidated with stakeholders to ensure they still provide value. The security measurement cycle is iterative and should be continuously refined to improve the effectiveness of the cyber risk program. By focusing on KPIs and KRIs, security practitioners can provide meaningful and relevant information to decision-makers, helping to improve the organization's cybersecurity posture.The threat landscape evolves, so security must also evolve. It's important to have the ability to fail fast, move on, and improve or repurpose to succeed in measuring cybersecurity.

About the Author

Steve Durbin is Chief Executive of the Information Security Forum, an independent, not-for-profit 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. Find out more at www.securityforum.org.

https://www.linkedin.com/in/stevedurbin/
https://www.securityforum.org/spotlight-on/

Steve Durbin

ISF

INFORMATION SECURITY FORUM (ISF)

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit organisation with a Membership comprising many of the world's leading organisations featured on the Fortune 500 and Forbes 2000 lists. It is 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

Threat Horizon 2025

Scenarios for an uncertain future

1

The Future of Work: Location and technology collide

- 1.1 Outsourcing everything
- 1.2 The fake employee
- 1.3 The good old days
- 1.4 Rise of the machines

2

The Future of Data: Regulation plays catch-up with value

- 2.1 Sweating the data assets without a moral compass
- 2.2 The rebellious data curator
- 2.3 The desperate data fisherman
- 2.4 The sleepwalking data hoarder

3

The Future of International Relations: Ideologies clash in the hyperconnected world

- 3.1 Regulation sours special relationships
- 3.2 Digitised utopia
- 3.3 Technological Dystopia
- 3.4 Hostile embraces

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

With a community of over 20,000 information security professionals, we are the recognised authority on cyber, information security and risk management.

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:

Kiersten Todt, Marina Kaljurand, Geoff Brown, Christopher Ahlberg, Valentin Weber, Fabian Bahr, Wolfgang Baare-Schmidt, Eva Mattes, Alexander Schellong, Tobias Kiesling, Doris Groot, Christopher McKinney, Thomas Tarantino, Stefan Lankes, June Chambers, Jens Redmer, Koh Nakaji, Shinichi Yokohama, Franziska Armbruster, Marina Hoffmann, Marina Geigenberger, Nick Kelly, Detlef Houdeau, Christine Schmerber, Matthias Bandemer, Tobias Lang, Victor del Razo, Harald Gossner, Sergej Epp, Kai Horten, Kristyn Ha, Kai Hermsen, Christine Lynch, Veronika Reichl, Nadine Tschersich, Julia Walter, Tomoyuki Kishi, Kathrin Wagenhuber, Paul Desprez, Robert Kosla

This conference was organised by:

Peter Moehring
Managing Director
Security Network Munich
Giesecke+Devrient

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

Lorenz Hoeppl
Assistant to the
Managing Director
Security Network Munich

Marc Raimondi
Chief of Staff at
Silverado Policy
Accelerator
(Washington D.C.)

Christopher Krebs
Founding Partner of
the Krebs Stamos Group
(Washington D.C.).

SECURITY NETWORK MUNICH
Europe's leading expert network for information security

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

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

For more information on the network and membership, please visit https://it-security-munich.net.

Security Network Munich