Security Network
Munich

@SN_Munich
#MCSC24

SECURITY NETWORK MUNICH
PRESENTS

MCSC

MUNICH CYBER SECURITY CONFERENCE 2024

10TH ANNIVERSARY

Where To From Now?

Ways Forward Out Of The Cyber Conundrum

Chamber of Commerce Munich (IHK)
15/16 February 2024

Patronized by:

Bavarian Ministry of Economic Affairs,
Regional Development and Energy

Supported by:

AIRBUS · paloalto NETWORKS · Giesecke+Devrient Creating Confidence · EY Building a better working world · accenture

BRUNSWICK · SIDLEY · Meta · aws · Google · TikTok

infineon · SentinelOne · Recorded Future · WITH secure · Lenovo

Distinguished Guests,

Welcome to Munich, Welcome to the 10th Anniversary Edition of MCSC.

10 years MCSC and Cybersecurity has not lost an inch of relevance since its inception. Rather the contrary, it is more relevant than ever to discuss the urgencies and latest developments on cyber risks and how to counter them, but even more so, to find ways in improving coordination and collaboration across countries and boundaries of public and private sectors for becoming more efficient and successful in our effort.

We need forums like the MCSC to do exactly that. The program reflects these developments and demanding challenges for achieving cyber readiness.

A sense of activism which is not coordinated in the best possible way lead us to the title of this years conference: Where to from Now? Ways forward out of the Cyber Conundrum.

Please do engage and offer your thoughts and expertise in making this special anniversary edition a success.

Thank you for coming, thank you for being part of this effort.

Yours sincerely

Security Network Munich

Claudia Eckert

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

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.

OPINION

Fighting Fire with Fire: Protecting 2024 Elections Intelligently

Christopher Ahlberg

Co-Founder and CEO of Recorded Future (Washington D.C.)

Over the last 25 years, the internet has become a reflection of the world. Over the next 25 years the world will become a reflection of the internet - in all the fundamental aspects of society - democracy, power, identity, money, culture, and more.

The internet promised to unlock freedom and democracy in countries such as China, Russia, Iran, and the Arab world. In reality, it has gone the opposite way. Authoritarians love the internet. They can communicate without middlemen, filter and shape the information their citizens see, and shut off information flows when necessary – freed from the shackles of traditional media. The advent of artificial intelligence presents authoritarian leaders with unparalleled means to exert control over their populace and project influence on a global scale. In 2016, Russian President Vladimir Putin effectively employed the Internet Research Agency, a St. Petersburg-based entity, to sway Western audiences. With AI capabilities, manipulation can now be automated with ease. Consequently, imminent elections globally are faced with daunting prospects, including an onslaught of large-scale TikTok memes or meticulously crafted deep fakes, engineered by nefarious AI systems, disseminated across digital platforms.

However, there is hope: Intelligence can be deployed to combat authoritarians, where intelligence not only guides the bullet but becomes the munition itself. To achieve this, a faster pace and collaboration among parties that historically haven't worked together are necessary. In the early stages of the Russian invasion of Ukraine, American and British intelligence agencies broke tradition by publicly revealing Russian plans to invade Ukraine in real time. This departure from standard practice, where such sensitive information would typically remain undisclosed due to source protection, marked a significant shift. While this disclosure was helpful, the bureaucratic processes for declassifying government intelligence remain slow and complex, lacking the speed necessary to address immediate threats to democracy and elections. As the internet becomes the primary tool for gathering intelligence, private entities can respond more quickly, accessing and interpreting information in a similar manner to government agencies. During a collaborative effort with Ukrainian agencies, Recorded Future helped to identify and expose Russian intelligence command and control systems deployed to infiltrate the Ukrainian Prosecutors Office. The operation, spanning five days, aimed to uncover potential targets for war crime trials. By establishing a joint intelligence network connecting private intelligence in various sectors of the Ukrainian government, we were able to facilitate continuous updates to our AI algorithms and detect and verify evidence of Russian intrusions with Ukrainian authorities. This pace and nature of public-private collaboration across national borders will be critical to protect democracy in an internet centric world.

Fighting fire with fire. As disinformation campaigns persist, they threaten to undermine trust in democratic processes, manipulate public opinion, exacerbate social division and polarization, and endanger national security. These campaigns distort reality, sow confusion, and erode the foundations of democracy, ultimately compromising the integrity of electoral processes and threatening the legitimacy of democratic governance. The West and its allies must adopt a new form of intelligence that integrates cyber warfare and disinformation responses, leveraging connectivity and AI at its core rather than relying solely on outdated methods. This approach, often termed "open source intelligence," demands a shift towards faster, more agile strategies to counter the rapid integration of technology and disinformation. Organizations like Bellingcat employ internet-based intelligence to expose the identities of malicious actors such as Russian spies accused of murder. The challenge and opportunity lies in harnessing the same internet used by malicious actors to collect intelligence and conduct analysis through AI-based algorithms. By integrating privacy safeguards directly into the intelligence cycle, we can demonstrate that these measures better protect individual privacy than traditional methods while effectively countering disinformation and cyber threats.

As we envision the future beyond 2024, I remain optimistic. Safeguarding elections globally demands novel forms of collaboration between governments and private intelligence providers. Government entities have unique authorities to perform intelligence-gathering activities that remain important. Combining insights gained from such methods with internet based intelligence gained in real time can empower democracies to identify and counteract bad actors, disinformation campaigns, and their underlying sponsors in ways and at a pace that will put our adversaries on the back foot. We must remain vigilant through of the various paths that may lead us astray. Earlier this year, a group of technologists, including Elon Musk, called on "AI labs to immediately pause for at least six months the training of AI systems more powerful than GPT-4 to prevent losing 'control of civilization.'" Such a pause would surely allow our adversaries, especially during the crucial election year of 2024, to gain an advantage. We could make an unwise decision by prohibiting the use of AI and intelligence in espionage and warfare, particularly as Russian and Chinese intelligence agencies gain access to Western AI platforms and use them against us. Intelligence will play a critical role in protecting our values in 2024 and beyond. Our adversaries are already capitalizing on the current landscape, and despite any discomfort we may feel, we must respond in kind. Embracing AI becomes imperative as a means to counter those who seek to exploit it against us.

MUNICH CYBER SECURITY CONFERENCE (MCSC) 2024

Where To From Now? Ways Forward Out Of The Cyber Conundrum

THURSDAY, FEBRUARY 15TH

2:00–2:05 p.m.	**Welcome**	**Claudia Eckert** Chairwoman of Security Network Munich (Munich)
2:05–2:10 p.m.	**Greeting**	**Georg Eisenreich** Bavarian State Minister of Justice (Munich)
2:10–2:20 p.m.	**10 Years MCSC**	**Ralf Wintergerst** Former Chair of Security Network Munich, President of Bitkom, Group CEO of G+D (Munich)
2:20–2:35 p.m.	**Opening Keynote**	**Margaritis Schinas** Vice President of the EU Commission (Brussels)
2:35–2:45 p.m.	**Special Thanks**	**Despina Spanou** Head of Cabinet for European Commission Vice President Margaritis Schinas (Brussels) **Kiersten Todt** CEO and Managing Partner at Liberty Group Ventures, LLC (Washington D.C.)
2:45–3:00 p.m.	**Fireside Chat** **Moderator: Dmitri Alperovitch** Executive Chairman at Silverado Policy Accelerator (Washington D.C.)	**Anne Neuberger** Deputy Assistant to the President & Deputy National Security Advisor for Cyber & Emerging Technologies at The White House (Washington D.C.)
3:00–3:50 p.m.	**First Panel:** Where to from now? A Cyber Strategy Update. **Moderator: Arthur de Liedekerke** Senior Director for European Affairs at Rasmussen Global (Brussels)	**Katherine Getao** Former CEO at ICT Authority of Kenya (Nairobi) **Nicola Hudson** Partner and Cybersecurity, Data & Privacy Global Lead at Brunswick Group (London) **Florent Kirchner** Head of the National Cybersecurity Strategy, Services of the Prime Minister, France (Paris) **Sami Khoury** Head of the Canadian Centre for Cyber Security (Ottawa) **Matthew Collins** Deputy National Security Advisor of the UK (London) **Jake Braun** Acting Principal Deputy National Cyber Director (Washington D.C.)
3:50–4:25 p.m.	**Coffee Break**	
4:25–4:40 p.m.	**Keynote**	**Chris Wray** Director of the FBI (Washington D.C.)

4:40–5:30 p.m.	**Second Panel:** Democracy under Stress: Collision of Elections and Disinformation. **Moderator: Vivian Schiller** VP and Executive Director at The Aspen Institute (Washington D.C.)	**Olga Belogolova** Director of the Emerging Technologies Initiative at John Hopkins University (Washington D.C.) **Sandra Joyce** VP Mandiant Intelligence at Google Cloud (Washington D.C.) **David Agranovich** Director for Global Threat Disruption at Meta (San Francisco) **Nick Beim** Partner at Venrock (New York) **Theo Bertram** Vice President, Government Relations and Public Policy for Europe at TikTok (London)
5:30–6:00 p.m.	**Spot-on:** Limits of Control: An Intelligence View on Cyber. **Moderator: Christopher Ahlberg** CEO of Recorded Future (Washington D.C.)	**Sir Alex Younger** Former Chief of Secret Intelligence Service MI6 (London) **Sir Jeremy Fleming** Former Head of UK Intelligence Agency, GCHQ (London)
6:00–6:35 p.m.	**Coffee Break**	
6:35–7:25 p.m.	**Third Panel:** The Cyber Policy Dilemma: Regulation-Curse or Blessing for Business? **Moderator: Siobhan Gorman** Partner and Cybersecurity, Data & Privacy Global Lead at Brunswick Group (Washington D.C.)	**Claudia Plattner** President of the German Federal Office for Information Security (Bonn) **Julie Teigland** Managing Partner, EY EMEIA (London) **Siegfried Russwurm** President of the Federation of German Industries (BDI) (Berlin) **Pascal Andrei** Chief Security Officer of Airbus (Toulouse) **Lorena Boix Alonso** Director for Digital Society, Trust & Cybersecurity at European Commission (Brussels)
7:25–7:45 p.m.	**Guest of Honor** **Moderator: Maia Mazurkiewicz** Co-Founder & Head of StratCom, Alliance4Europe (Warsaw)	**Sviatlana Tsikhanouskaya** Opposition Leader Belarus (Minsk)
7:45 p.m.	**Greeting and Reception Party** **Moderator: Oliver Rolofs** Co-Founder of MCSC (Munich)	**Tobias Gotthardt** Bavarian State Secretary for Economic Affairs, Regional Development and Energy (Munich) **Ambassador Wolfgang Ischinger** President of the Foundation Council, Munich Security Conference Foundation (MSC-Chairman 2008-2022) (Munich)

FRIDAY, FEBRUARY 16TH

8:00–8:30 a.m.	**Coffee Hour**	
8:30–8:45 a.m.	**Keynote**	**Alejandro N. Mayorkas** U.S. Secretary of Homeland Security (Washington D.C.)
8:45–8:55 a.m.	**Vantage Point**	**Kazutaka Nakamizo** Deputy Director General of the NISC, Japan (Tokyo)
8:55–9:45 a.m.	**Fourth Panel:** (IoT) Security by Design – Illusive, or will Norms and Standards prevail? **Moderator: Kiersten Todt** CEO and Managing Partner at Liberty Group Ventures, LLC (Washington D.C.)	**Luis Jorge Romero** Director General of ETSI (Sophia Antipolis) **Katerina Megas** Cybersecurity for IoT Program Lead at NIST (Sterling) **Vincent Strubel** Director General of ANSSI (Paris) **Peter Stephens** Former Head of UK's "Secure by Design" Initiative (Paris) **Samantha Kight** Head of Industry Security at the GSMA (London) **Thomas Rosteck** Division President Connected Secure Systems at Infineon (Munich)
9:45–10:15 a.m.	**Talking Heads** **Moderator: Jeff Moss** President and Founder of DEF CON (Washington D.C.)	**Kemba Walden** President of the Paladin Global Institute and Former Acting U.S. National Cyber Director (Washington D.C.) **Bruce Schneier** Fellow and Lecturer Harvard Kennedy School (Cambridge, MA)
10:15–11:05 a.m.	**Fifth Panel:** Intersection of AI and Cybersecurity. **Moderator: Katie D'Hondt Brooks** Director Global Cybersecurity Policy at Aspen Digital (Washington D.C.)	**Koos Lodewijkx** CISO for IBM (Washington D.C.) **Heather Adkins** Vice President Security Engineering at Google (Mountain View) **Jason Ruger** CISO at Lenovo (Chicago) **Paul Vixie** VP and Deputy CISO at AWS (Redwood City) **Jonas Andrulis** Founder and CEO of Aleph Alpha (Heidelberg)
11:05–11:20 a.m.	**Closing Moderated Keynote** **Moderator: John Carlin** Partner at Paul Weiss (Washington D.C.)	**Lisa Monaco** Deputy Attorney General of U.S. (Washington D.C.)
11:20–11:55 a.m.	**Coffee Break**	

11:55–12:45 a.m.	**Sixth Panel:** Where the Money is –Insights from the Champions of Risk Management. Moderator: **Wolfram Seidemann** CEO at G+D Currency Technology (Munich)	**Cheryl Venable** EVP, Chief of Payment Operations, Federal Reserve Bank of Atlanta (Marietta) **Cheri McGuire** Chief Technology Officer at Swift (Virginia) **Ronald Green** Cybersecurity Fellow and Former Chief Security Officer at Mastercard (St. Louis) **Rafael Garcia Oliva** Deputy Director General in the Directorate General Information Systems at ECB (Frankfurt) **Sergej Epp** Chief Security Officer EMEA Central at Palo Alto Networks (Frankfurt)
12:45–12:50 p.m.	**World View** on Public-Private Partnerships	**Akihiro Wada** Chair of Working Group at Committee on Cyber Security, Keidanren (Tokyo)
12:50–1:40 p.m.	**Seventh Panel:** Connecting Dots in Cyber Defense. Moderator: **David Lashway** Partner at Sidley (Washington D.C.)	**Emily Goldman** U.S. Cyber Command (Washington D.C.) **Manfred Boudreaux-Dehmer** NATO Chief Information Officer (Brussels) **Pekka Jokinen** Director at National Cyber Security Center Finland (Helsinki) **Michael Rogers** Admiral (ret.) U.S. Navy (New York) **Alexander Klimburg** Senior Fellow at The Hague Center for Strategic Studies (The Hague)
1:40 p.m.	**End**	

INSTITUTIONAL PARTNERS:

msc Munich Security Conference

CYBER READINESS INSTITUTE

Aspen Institute Germany

UNITED EUROPE competitive and diverse

Bundesamt für Sicherheit in der Informationstechnik

BSA The Software Alliance

ISF

CSSA Cyber Security Sharing & Analytics

bitkom

Charter of Trust

DsiN Deutschland sicher im Netz

invest in bavaria

BDI

ECS European Cyber Security Organisation

German Mittelstand

Keidanren Policy & Action

bayern innovativ Innovation leben.

ZD.B Cyber-Security

ASPEN DIGITAL aspen institute

Alliance 4Europe

DGAP Advancing foreign policy. Since 1955.

EnSure collaborative

DIGITALEUROPE

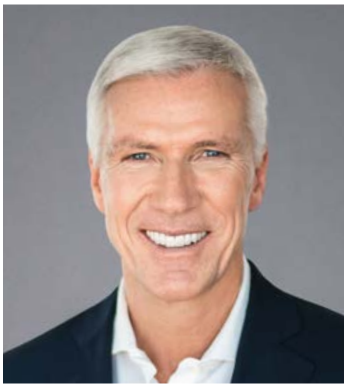
DISTINGUISHED GUEST OF HONOR

Sviatlana Tsikhanouskaya

Opposition Leader Belarus (Minsk)

Sviatlana Tsikhanouskaya is a National Leader of Belarus and a Head of the United Transition Cabinet of whom independent observers agree won the presidential election on August 9, 2020, against the long-lasting dictator Aliaksandr Lukashenka. After the start of Russian invasion of Ukraine in February 24th, 2022, Tsikhanouskaya reformatted the leadership of the movement by creating and chairing the United Transition Cabinet, the decision-making center of the movement. Led by Tsikhanouskaya, Belarusian anti-war activists conducted underground resistance in Belarus by sabotaging railway transportation of Russian troops as well as volunteering Belarusian-staffed units fighting for Ukraine. As the leader of the Belarusian democratic movement, she has visited 28 countries, gathering support and advocating for the release of more than 1500 of political prisoners and a peaceful transition of power through free and fair elections. In meetings with President Biden, Chancellor Merkel, President Macron, President von der Leyen, President Charles Michel, Prime Minister Trudeau and other world leaders, Tsikhanouskaya emphasized the need for a braver response to the actions of the Belarusian dictatorship. Tsikhanouskaya's story began when she entered the race after her husband Siarhei Tsikhanousky was arrested for voicing his presidential aspirations. Lukashenka publicly dismissed her as a "housewife," saying that a woman cannot become president. Nonetheless, Tsikhanouskaya united and successfully led the democratic coalition. Following her forced exile, Sviatlana Tsikhanouskaya inspired unprecedented peaceful protests in Belarus, with some rallies numbering hundreds of thousands people. When the war has started, Sviatlana Tsikhanouskya announced the anti-war movement to prevent the participation of Belarus in the war against Ukraine. Mass campaign of disobedience and dozens acts of sabotage took place aimed to stop Russian troops from entering Ukraine from Belarus territory. In 2020–2023, Sviatlana Tsikhanouskaya became a symbol of the peaceful struggle for democracy and strong female leadership. Among dozens of distinctions, she is a recipient of the Sakharov Prize awarded by the European Parliament, 2022 International Four Freedoms Award, and Charlemagne Prize. In 2021 and 2022, she was nominated for the Nobel Peace Prize by Lithuanian President Gitanas Nauseda and Members of the Norwegian Parliament respectively. Tsikhanouskaya has been recognized in Bloomberg's Top 50 Most Influential People, Financial Times' Top 12 Most Influential Women, and Politico's Top 28 Most Influential Europeans.

10 YEARS MCSC:



Ralf Wintergerst

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

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 Services departments of Information Systems, Corporate Security, Compliance Management and Auditing, Corporate Communications, Mergers & Acquisitions, Corporate Strategy, Corporate Development, Legal Services, and Corporate Governance. Wintergerst joined G+D in 1998 and has held various management positions in the company. He became a member of the Management Board in 2013 with his appointment to lead the business unit Banknote (today Currency Technology). In 2016 he was named Chairman of the Management Board and CEO of G+D. Alongside his role at G+D, Wintergerst is president of the German digital association Bitkom. Furthermore, he is Chairman of the Supervisory Board of secunet Security Networks AG (Essen, Germany) and President of the Board of Directors of netcetera AG (Zurich, Switzerland). 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

Claudia Eckert

Chairwoman of Security Network Munich (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.

Georg Eisenreich

Bavarian State Minister of Justice (Munich)

Georg Eisenreich studied law at LMU Munich and has been a licensed lawyer in Munich since 2001 (currently not exercised due to a public office). Georg Eisenreich has been a member of the Bavarian Landtag (State Parliament) since 2003. From 2013 to 2018, he was Bavarian Vice-Minister for Education and Religious Affairs, Science and the Arts, from March to November 2018 Bavarian State Minister for the Digital Agenda, Media and Europe. Georg Eisenreich was appointed Minister of Justice on November 12, 2018.

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.

SPEAKERS

Despina Spanou

Head of Cabinet for European Commission Vice President 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.

Kiersten E. Todt

CEO and Managing Partner at Liberty Group Ventures LLC (Washington D.C.)

Kiersten Todt is the former Chief of Staff of the Cybersecurity and Infrastructure Security Agency (CISA). In that role, she was responsible for the planning, allocation of resources, and development of long-range objectives in support of the department's goals. She oversaw the management and execution of an almost $3B budget. She currently serves in an advisory role to CISA's Director. She is also a strategic advisor to venture capital firms and to the Data and Trust Alliance, which is a CEO-led cross-sector industry effort to create standards for data provenance and high-risk use of artificial intelligence. She also serves on Boards of technology companies, which are focused on open source software, memory safe language, and neurodiversity. Prior to her role at CISA, Kiersten was the Managing Director of CRI, a non-profit that develops free cybersecurity tools for small businesses, worldwide. She co-founded CRI with the CEOs of Mastercard, Microsoft, PSP Partners, and the retired CEO of IBM. As CEO of Liberty Group Ventures, she has worked extensively with senior leaders in industry on cyber risk management. Her service to the Federal Government includes serving as a professional staff member in the U.S. Senate, co-drafting the legislation to create the Department of Homeland Security, and as Executive Director of President Obama's Commission on Enhancing National Cybersecurity.

Arthur de Liedekerke

Senior Director for European Affairs at Rasmussen Global (Brussels)

Arthur de Liedekerke is Senior Director for European Affairs at political advisory Rasmussen Global and a non-resident fellow at the Institute for Security Policy at Kiel University (ISPK). He has previous experience advising senior officials in the French Ministry for the Armed Forces and the institutions of the European Union (Commission and Parliament) on security and defence matters. He holds a master's degree in international relations from the University of Maastricht and a master's in geopolitics from King's College London. He is regularly featured and published in francophone and international media outlets including Le Monde, Les Echos, La Tribune, La Libre Belgique, Politico, and Sky News among others.

SPEAKERS

Anne Neuberger

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

Ms. Neuberger is the Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technologies in the White House. Previously, she served at the National Security Agency (NSA) for over ten years in a variety of senior intelligence and cybersecurity roles. Most recently, she served as director of NSA's Cybersecurity organization and deputy director of NSA's intelligence operations, leading an organization of over 20,000 people globally. In both these roles, she drove major change initiatives across operations and technology. She also served as NSA's first Chief Risk Officer building NSA's enterprise risk management program and Director of NSA's Commercial Solutions Center, which leads its private sector outreach. Prior to NSA, she served as the Department of the Navy's Deputy Chief Management Officer and a White House Fellow in the Office of the Secretary of Defense. In 2020, Ms. Neuberger was awarded DoD's and NSA's highest civilian awards, the DoD Distinguished Civilian Service Award, and NSA's Distinguished Service Medal. In 2017, Ms. Neuberger was awarded a Presidential Rank Award. Before her government service, Ms. Neuberger was Senior Vice President of Operations at American Stock Transfer and Trust Company, where she directed technology and operations. Ms. Neuberger is a graduate of Columbia University, where she earned an MBA and Masters of International Affairs.

Dmitri Alperovitch

Executive Chairman at Silverado Policy Accelerator (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 2021, he launched the Alperovitch Institute for Cybersecurity Studies at Johns Hopkins University's School of Advanced International Studies (SAIS). Alperovitch was also named a "D.C. Tech Titan" and one of the 500 most influential people in Washington by Washingtonian Magazine in 2022 and 2023. He is the host and creator of Silverado's popular "Geopolitics Decanted" podcast, dedicated to expert analysis of the war in Ukraine and broader geopolitical and national security issues including developments on semiconductor and AI policy. In 2023, DHS Secretary Alejandro N. Mayorkas presented Alperovitch with the Outstanding Americans by Choice recognition for his civic and professional contributions as a naturalized U.S. citizen.

SPEAKERS

Katherine W. Getao

Former CEO at ICT Authority of Kenya (Nairobi)

Dr. Katherine W. Getao, EBS, is often dubbed an “ICT Elder” in Kenya, in recognition of her 40 years of service in the private sector, academia, diplomacy as well as senior government appointments. Dr. Getao currently executes consultancy assignments in the areas of Cyber Hygiene, Cyber Diplomacy and ICT Strategy and Governance. She has served as the Chief Executive Officer of the ICT Authority in Kenya, the ICT Secretary in the Office of the President and subsequently at the Ministry of ICT. During her time in government, she led the design of the Huduma Centre one-stop shops for government services as well as the integrated implementation of optical fibre in collaboration with the Roads sector. Project Manager of the NEPAD e-Schools Project as well as the Director of the School of Computing and Informatics at the University of Nairobi. She has represented Kenya on UN Governmental Committees and has also served on the boards of private companies and universities. Dr. Getao is passionate about public service transformation using ICTs and the creation of industries and career opportunities for young people in the ICT Sector. Dr. Getao serves on a high-level global think tank, the Aspen Global Group, and also as a regional adviser to the Diplo Foundation.

Nicola Hudson

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

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.

Florent Kirchner

Head of the National Cybersecurity Strategy, Services of the Prime Minister, France (Paris)

Florent Kirchner is the Head of the French Cybersecurity Strategy, within the Prime Minister’s services, and is tasked with planning and coordinating investments nation-wide and in connexion with European initiatives. In practice, this means -- among other things -- funding research, innovation, operations, incubators, commons, ecosystems, and training with the aim to building a better, more trustworthy digital future. This is part of the France2030 plan, a 54B€ investment effort overall. He holds a Masters from ENS and a Ph.D from Ecole Polytechnique, both in computer science and formal methods. He worked with amazing people at SRI International, Inria, and CEA; managed one of the largest teams of applied research in software and systems engineering, and coordinated the SPARTA EU pilot program as its Strategic Director. He had the priviledge of becoming an auditor at IHEDN, in the 3rd session "souveraineté numérique et cybersécurité". Florent Kirchner is interested in supporting cyber-diversity in all its forms, in unexpected collaborations, in emerging trends – and old resurgences.

SPEAKERS

Sami Khoury

Head of the Canadian Centre for Cyber Security (Ottawa)

Sami Khoury is the Head of the Canadian Centre for Cyber Security (the Cyber Centre). The Cyber Centre is the single unified source of expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public. Sami began his career at the Communications Security Establishment (CSE) in 1992 as a research engineer exploring the impact of emerging multimedia communications technologies. He held various management positions and leadership roles at CSE, including Director General Capabilities Development and more recently as Deputy Chief (ADM) for Enterprise Technologies and Solutions. In this role, he was CSE's Chief Information Officer (CIO) and responsible for IT and Information Security, as well as leading CSE's overall Research program and 24/7 Operations Centre. Sami holds a Bachelor of Computer Engineering (1988) and a Masters of Applied Science (1991) from Concordia University in Montreal. He completed a certificate program in Public Sector Leadership at the University of Ottawa in 2016. Sami received the Queen Elizabeth Diamond Jubilee Medal in 2012 and the APEX Award of Excellence for Innovation in 2020.

Jake Braun

Acting Principal Deputy National Cyber Director (Washington D.C.)

Jacob (Jake) Braun serves as Acting Principal Deputy National Cyber Director in the White House. Previously he served as Senior Counselor for Transformation to The Secretary of Homeland Security. He was initially appointed by President Joseph Biden as Senior Advisor to the Department of Homeland Security's Management Directorate in February of 2021. He is also a lecturer and former Executive Director of the Cyber Policy Initiative at the University of Chicago Harris School of Public Policy. He works at the center of politics, technology, and national security. He is the author of the book, Democracy in Danger: How Hackers and Activists Exposed Fatal Flaws in the Election System and has co-authored three award-winning and seminal works on election infrastructure cyber vulnerabilities. Mr. Braun was Chief Executive Officer of Cambridge Global Advisors from 2013-2021. He assisted clients in the management, development, and implementation of their national security programs, practices, and policies with a focus on cyber security. Prior to joining the University of Chicago Harris School of Public Policy faculty and Cambridge Global Advisors, Mr. Braun was appointed by President Barack Obama as Director of White House and Public Liaison to the Department of Homeland Security where he oversaw some of the most high-profile public engagements executed at DHS. He was instrumental in the effort to gain passage in the European Parliament of the largest data sharing agreement between the United States and the European Union. In addition, he designed and implemented a program to modernize the DHS cybersecurity workforce. Mr. Braun also oversaw stakeholder crisis communications for the White House during the 2010 Deep Water Horizon Gulf Oil Spill. Prior to his tenure as White House Liaison, Mr. Braun served on the Presidential Transition Team for the Obama Administration as Deputy Director for the National Security Agencies Review. In this capacity he oversaw agency review programs for all national security agencies including the State Department, DOD, DHS, CIA, USAID, etc. and guided policy assessments from their inception to the then-President-Elect's desk. Mr. Braun is also co-founder of the DEF CON Voting Machine Hacking Village, and in the President's Circle on the Chicago Council on Global Affairs. Mr. Braun began his career as a journalist for newspapers in Illinois and Taiwan. He holds an MA in International Relations from Troy St. University, an MA in Education from National-Louis University in Chicago, and a BA in Philosophy from Loyola University of Chicago.

SPEAKERS

Matthew Collins

Deputy National Security Advisor of the UK (London)

Matt Collins is the Deputy National Security Adviser - Intelligence, Defence and Security in the Cabinet Office.Matt has been in the Civil Service for 17 years, most recently in his role as Director for Intelligence, Technology and Security within the National Security Unit in the Cabinet Office. The portfolio covered counter-terrorism and serious and organised crime, oversight of intelligence finance, critical and emerging technology and digital, data and intelligence policy. Matt is a one-time professional basketball player, a keen runner and cyclist and has an MSc in Criminology from the London School of Economics.

Christopher Wray

Director of the FBI (Washington D.C.)

Christopher Wray became the eighth Director of the FBI on August 2, 2017. Mr. Wray began his law enforcement career in 1997, serving in the Department of Justice as an assistant U.S. attorney for the Northern District of Georgia. In that role, Mr. Wray prosecuted a wide variety of federal criminal cases, including public corruption, gun trafficking, drug offenses, and financial fraud. In 2001, Mr. Wray was named associate deputy attorney general, and then principal associate deputy attorney general, in the Office of the Deputy Attorney General in Washington, D.C. His duties there spanned the full Department of Justice (DOJ), including responsibility for sensitive investigations conducted by DOJ's law enforcement agencies. Mr. Wray was nominated by President George W. Bush in 2003 to be the assistant attorney general for DOJ's Criminal Division, supervising major national and international criminal investigations and prosecutions. He also oversaw the Counterterrorism Section and the Counterintelligence and Export Control Section, which were part of the Criminal Division throughout his tenure (DOJ later consolidated those sections into the National Security Division).Mr. Wray was a member of the President's Corporate Fraud Task Force, supervised the Enron Task Force, and served as a leader in DOJ's post-9/11 efforts to combat terrorism, espionage, and cybercrime with domestic and foreign government partners. At the conclusion of his tenure, Mr. Wray was awarded the Edmund J. Randolph Award, DOJ's highest award for leadership and public service. Mr. Wray was born in New York City. He graduated with a bachelor's degree from Yale University in 1989 and earned his law degree from Yale Law School in 1992. He clerked for Judge J. Michael Luttig of the U.S. Court of Appeals for the Fourth Circuit. In 1993, Mr. Wray joined the international law firm of King & Spalding LLP, where he spent a total of almost 17 years practicing law in the area of government investigations and white-collar crime. At the time of his nomination to be FBI Director, Mr. Wray was chair of the firm's Special Matters and Government Investigations Practice Group.

David Agranovich

Director for Global Threat Disruption at Meta (San Francisco)

David Agranovich is Meta's Director of Threat Disruption, where he coordinates the disruption of influence operations, cyber-espionage, and adversarial networks across Meta and develops policies to deter misuse of the platform. Prior to joining Facebook, David served as Director for Intelligence at the National Security Council (NSC) in the White House, where he led the United States Government's efforts to address foreign interference in democratic systems and elections and in a variety of senior roles at the Department of Defense focused on Russian counter-intelligence, organized crime and corruption. In his free time he is a commercial pilot and flight instructor.

SPEAKERS

Olga Belogolova

Director of the Emerging Technologies Initiative at John Hopkins University (Washington D.C.)

Olga is the Director of the Emerging Technologies Initiative at the Johns Hopkins School of Advanced International Studies (SAIS). She also professor at the Alperovitch Institute for Cybersecurity Studies at SAIS, where she teaches on disinformation and influence in the digital age. At Facebook/Meta, she led policy for countering influence operations, leading execution and development of policies on coordinated inauthentic behavior, state media capture, and hack-and-leaks within the Trust and Safety team. Prior to that, she led threat intelligence work on Russia and Eastern Europe at Facebook, identifying, tracking, and disrupting coordinated IO campaigns, and in particular, the Internet Research Agency investigations between 2017-2019. Olga previously worked as a journalist and her work has appeared in The Atlantic, National Journal, Inside Defense, and The Globe and Mail, among others. She is a fellow with the Truman National Security Project, serves on the review board for CYBERWARCON, the Trust & Safety Advisory Group of the Institute for Security and Technology, and is on the board of directors for the Digital Democracy Institute of the Americas (DDIA).

Sandra Joyce

VP Mandiant Intelligence at Google Cloud (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. Sandra 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 the Board of Visitors at National Intelligence University. She is also 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.

Theo Bertram

Vice President, Government Relations and Public Policy for Europe at TikTok (London)

Theo Bertram is TikTok's Vice President of Government Relations and Public Policy for Europe. Theo is a member of TikTok's Europe management team and oversees all of TikTok's government relations and external affairs functions in the UK, Israel and throughout Europe. Prior to joining TikTok, Theo worked at Google for nearly a decade and led Google's public policy teams across Europe, Middle East, Africa and Russia. Prior to this, Theo served as O2 UK's Head of Public Affairs. Before working in the private sector, Theo had extensive political and governmental experience having served as a Special Adviser and Head of Research and Information to British Prime Ministers Tony Blair and Gordon Brown. He worked in the Campaigns and Communication team within the Labour Party from 2000 to 2006. Theo earned his PhD in English Literature from the University of Bristol in 2000.

SPEAKERS

Nick Beim

Partner at Venrock (New York)

Nick Beim is a partner at Venrock, the venture capital firm created by the Rockefeller family that helped pioneer the venture capital industry. He focuses primarily on artificial intelligence, software, financial technology and defense. Beim serves on the boards of directors of companies including Dataminr, an AI platform that identifies critical breaking information from publicly available data; Rebellion Defense, which develops AI-driven products that serve the mission of national defense; Percipient.ai, an advanced computer vision analytics platform; Interos, a multi-factor, multi-tier risk management platform; and Altruist, a digital investment platform for financial advisors. Beim serves on the board of directors of the Council on Foreign Relations and of Endeavor, a nonprofit that supports high-impact entrepreneurs globally. He serves on the executive advisory committee of the Center on Global Energy Policy. He previously worked at Matrix Partners, Goldman Sachs, and McKinsey & Company. He received a BA in philosophy from Stanford University and an MPhil in international relations from Oxford University, where he was a Marshall Scholar.

Vivian Schiller

VP and 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.

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

Sir Jeremy Fleming

Former Head of UK Intelligence Agency, GCHQ (London)

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.

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.

Julie Linn Teigland

Managing Partner, EY EMEIA (London)

Julie is a member of the EY Global Executive and Area Managing Partner for Europe, Middle East, India and Africa (EMEIA). As EY EMEIA Area Managing Partner, Julie leads a geographic area comprising member firms with more than 150,000 people across 95 countries and representing combined revenues of over US$20b. In this role she is responsible for all four business units, including assurance, tax, consulting, as well as strategy and transactions. Julie joined EY in 2001, has served as lead partner for several Fortune 500 clients and previously held a number of leadership roles within the international practice, including Managing Partner for EY in Germany, Switzerland and Austria. Julie continues to serve clients as a senior advisor, contributing to large-scale transformation and change programs. Julie was recently named one of Fortune magazine's Most Powerful Women International. With three decades of experience in professional services for international clients, she believes that business has a responsibility in tackling global challenges and that growth must be sustainable and deliver value that will benefit all stakeholders. Julie is an active champion of women and the Global Leader for the EY Women. Fast forward initiative. Julie also serves on several boards across Europe and the US, such as JA Europe, the largest non-profit in Europe dedicated to preparing young people for employment and entrepreneurship, Atlantik Brücke and the American Council on Germany, both committed to building relationships between Germany, Europe and the US. Born in the US, Julie has accumulated over 30 years of international experience with terms in the Netherlands, Germany and now the UK. She studied business in Heidelberg, Frankfurt and Paris and qualified as a US Certified Public Accountant.

SPEAKERS

Claudia Plattner

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

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).

Pascal Andrei

Chief Security Officer of Airbus (Toulouse)

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 Chief Security Officer, 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 Dubaï. 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.

Lorena Boix Alonso

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

Lorena Boix Alonso is Director for Digital Society, Trust and Cybersecurity in the Directorate General for Communications Networks Content and Technology (DG CONNECT), at the European Commission. She is a member of the Executive and Management Board of the European Network and Information Security Agency (ENISA) and as well as the Commission representative in the Governing Board of the European Cybersecurity Competence Centre (ECCC) and a member of the Management Board of the Computer Emergency Response Team for the EU Institutions (CERT EU). In the context of the Horizon Europe Programme, she co-chairs the Cluster 1 "Health" and Cluster 3 ''Civil security for society'' and is as well a member of the board Innovative Health Initiative (IHI) Joint Undertaking. Formerly, she was Acting Director for Policy Strategy and Outreach and Head of Unit for Policy Implementation and Planning, in DG CONNECT at the European Commission. Previously, she was Deputy Head of Cabinet of Vice President Neelie Kroes, Commissioner for the Digital Agenda. During Ms Kroes' mandate as Commissioner for Competition, she commenced in October 2004 as a member of her cabinet and became Deputy Head of Cabinet in May 2008. She joined the European Commission Directorate-General for Competition in 2003. Prior to that, she has worked for Judge Rafael García Valdecasas, at the European Court of Justice, as well as Deputy Director and Legal Coordinator of the IPR-Helpdesk Project and in private practice in Brussels. She holds a Master of Laws from the Harvard Law School. She graduated in Law from the University of Valencia and then obtained a Licence Spéciale en Droit Européen from the Université Libre de Bruxelles.

Siegfried Russwurm

President of the Federation of German Industries (BDI) (Berlin)

Siegfried Russwurm was elected President by the BDI's (Federation of German Industries) general assembly without dissenting votes in November 2020. His term of office began with the year 2021. Siegfried Russwurm was born in June 1963 in Marktgraitz. He is married and has two adult children. In 1988, he completed his studies in manufacturing technology at the University of Erlangen-Nürnberg as a graduate engineer. There, he received his doctoral degree at the Chair of Applied Mechanics where he researched numerical simulation processes. In 1992, he joined Siemens AG, first as a production planner and project manager in the medical technology division, later in various management positions in the medical and industrial business in Germany and Sweden. In 2006, he was appointed Divisional Director in Medical Technology, and in January 2008 he became a member of the Managing Board of Siemens AG, where he was active until March 2017. During this time, he was responsible for all industrial issues, as Chief Technology Officer for Technology, for Healthcare and for Human Resources. His regional responsibilities at Siemens included Europe, Africa and the Middle East. Russwurm is active in various supervisory and advisory boards. Among other things he has been Chairman of the Shareholders' Committee and the Supervisory Board of Voith GmbH & Co KGaA since March 2019 and was elected Chairman of the Supervisory Board of Thyssenkrupp AG in October 2019. Russwurm was chairman of the North Africa Middle East Initiative of German Business (NMI) under the umbrella of the BDI from 2015 to 2017. From 2014 to 2017, he was chairman of the Platform Industry 4.0 of several BDI member associations, and from 2011 to 2017 member of the Restricted Board of the BDI member association of the mechanical engineering industry, VDMA.As Chief Human Resources Officer and Labor Director of Siemens AG, he was also a member of the presidential board of the Confederation of German Employers' Associations (BDA) from 2008 to 2010. Russwurm serves on the Executive Board of the National Academy of Science and Engineering (acatech) and on the Board of the German-Swedish Chamber of Commerce. Since 2009 he has been an honorary professor of mechatronics at the University of Erlangen-Nürnberg.

Siobhan Gorman

Partner and Cybersecurity, Data & Privacy Global Lead at Brunswick Group (Washington D.C.)

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 worked on corporate crisis across a range of industries, including financial services, healthcare, defense, entertainment, technology, and automotive. Siobhan has also led a range of cybersecurity, public affairs, litigation, and corporate reputation projects in the financial, retail, airline, and technology sectors. Tapping her longtime journalism experience, she regularly advises clients on media relations issues and conducts media training for executives. Siobhan was a member of the Senior Advisory Group for Harvard University’s Defending Digital Democracy Project, which is focused on preventing and mitigating cyberattacks on the election process. She was also member of the Advisory Committee for Brown University's Executive Master in Cybersecurity. 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. Prior to joining The Journal in 2007, Siobhan was a Washington correspondent for The Baltimore Sun covering intelligence and security. From 1998 to 2005, she was a staff correspondent for National Journal covering similar issues. She began her career as a researcher for a columnist at The Washington Post. Siobhan won the 2006 Sigma Delta Chi Award for Washington Correspondence for her coverage of the National Security Agency and in 2000 received a special citation in national magazine writing from the Education Writers Association. She has been nominated three times for the Pulitzer Prize and is a graduate of Dartmouth College. Siobhan was featured in Cybersecurity Venture's Women Know Cyber: 100 Fascinating Females Fighting Cybercrime, released in 2019.

SPEAKERS

Maia Mazurkiewicz

Co-Founder of Future Force Foundation (Warsaw)

Maia Mazurkiewicz is an expert in combating disinformation and behavioural change with over 15 years of experience in political management, foreign affairs and communications. She believes that we need a change in the way we communicate to bring more understanding between people. She is a co-founder of Alliance4Europe where she serves as Head of Strat-Comm. She founded the Future Force Foundation and is Vice President of the Free European Media Association. As co-founder of Keyboard Warriors in Poland, she fights against online disinformation. An attorney trained in Poland and the USA, she works with the DISARM Foundation on the disinformation research framework recommended by NATO and EU StratComm. She has worked with various NGOs on democratisation projects and worked at the Chancellery of the President of the Republic of Poland from 2011 to 2015.

Tobias Gotthardt

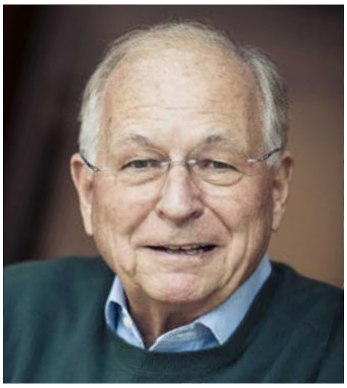
Bavarian State Secretary for Economic Affairs, Regional Development and Energy (Munich)

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.

Oliver Rolofs

Co-Founder of MCSC (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 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.



Wolfgang Ischinger

President of the Foundation Council, Munich Security Conference Foundation (MSC-Chairman 2008-2022) (Munich)

Ambassador (ret.) Wolfgang Ischinger was Chairman of the Munich Security Conference from 2008 until 2022 and is now President of the MSC Foundation Council. Wolfgang Ischinger looks back at a long diplomatic career including his role as State Secretary in the German Ministry of Foreign Affairs and posts as German ambassador in Washington D.C. and London.

Alejandro N. Mayorkas

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

Alejandro Mayorkas was sworn in as Secretary of the Department of Homeland Security by President Biden on February 2, 2021. A political refugee born in Havana, Cuba, Mayorkas is the first Latino and immigrant confirmed to serve as Secretary of Homeland Security. He has led a distinguished 30-year career as a law enforcement official and a nationally recognized lawyer in the private sector. Mayorkas served as the Deputy Secretary of the U.S. Department of Homeland Security from 2013 to 2016, and as the Director of U.S. Citizenship and Immigration Services from 2009 to 2013. Mayorkas began his government service in the Department of Justice, where he served as an Assistant United States Attorney in the Central District of California, specializing in the prosecution of white collar crime. After nearly nine years as a federal prosecutor, he became the youngest United States Attorney in the nation. Mayorkas received his bachelor’s degree with distinction from the University of California at Berkeley and a law degree from Loyola Law School.

Luis Jorge Romero

Director General of ETSI (Sophia Antipolis)

Luis Jorge Romero, Director General of ETSI, has 30 years of experience in the telecommunications sector. At ETSI he has initiated a global standardization partnership for IoT communications, oneM2M. He has overseen the rapid development of ETSI’s Industry Specification Groups accelerating market penetration of new technologies and has enabled the first Open Source group in ETSI, leading to the new Software Development Groups initiated in 2022. Luis Jorge has also successfully positioned the institute to take a leading role in 5G standardization through the 3GPP global partnership project and through initiatives such as ETSI’s Multi-access Edge Computing, Network Functions Virtualization or Reconfigurable Intelligent Surfaces groups. He is driving the implementation of the ETSI Strategy, an ambitious plan to prepare the institute for the future. Previously he has held diverse Director positions in Spain, Morocco and Mexico, predominantly with Telefonica. As Global Director for International Roaming and Standards, and Director of Innovation and Standards, he oversaw Telefonica's participation in global standardization activities, and participated directly in the work of the Next Generation Mobile Networks (NGMN) Alliance and in the GSM Association (GSMA). Before joining ETSI in July 2011, he held the position of Director General of Innosoft and was also a partner and board member of the Madrid-based Innology Ventures.

SPEAKERS

Kazutaka Nakamizo

Deputy Director General of the NISC, Japan (Tokyo)

In July 2023, he was appointed Deputy Director General of the NISC. Between 2021 and 2023, as Principal Counsellor of the NISC, he was responsible for the implementation and coordination of measures mentioned in the Cybersecurity Strategy adopted by the Cabinet in 2021. Before that, he was in charge of ICT-related policy at the Ministry of Internal Affairs and Communications, including security for telecommunications carriers and Internet service providers, protection of privacy and measures against disinformation on the Internet and standardization policies. Also, from 2012 to 2015, he worked at the Embassy of Japan in the United States as a telecom attaché. He joined Ministry of Internal Affairs and Communications (the former Ministry of Posts and Telecommunications) in 1993.

Katerina Megas

Cybersecurity for IoT Program Lead at NIST (Sterling)

Kat leads the NIST Cybersecurity for the Internet of Things (IoT) Program at the U.S. National Institute of Standards and Technology (NIST), focused on advancing and accelerating the development and application of research, standards, guidelines, and technologies necessary to improve the security and privacy of the ecosystem of connected devices. As the Program Manager she coordinates across the agency on all things related to cybersecurity of the IoT as well as leads a number of projects, including the NIST response on IoT for EO 13800, EO 14028 and the IoT Cybersecurity Improvement Act of 2020. Before joining NIST, Kat worked in the private sector for 25 years leading organizations in the development and execution of their IT strategies.

Vincent Strubel

Director General of ANSSI (Paris)

Vincent Strubel is a graduate from Ecole Polytechnique (class of 2000) and of Telecom ParisTech. In 2005, he started his career at the DCSSI (Central Network and Information Security Directorate), which later became ANSSI (French National Cybersecurity Agency). He successively held the positions of research lab manager, head of division and head of the Expertise department. In July 2020, he was appointed as head of the newly created OSIIC (Operator of Classified Interdepartmental Information Systems), which was a fusion of one of ANSSI's department and of the governemental transmission center (CTG). He held this position for two and a half years. General engineer Vincent STRUBEL was appointed Director General of ANSSI on January 4, 2023.

Peter Stephens

Former Head of UK's "Secure by Design" Initiative (Paris)

Peter Stephens is a former UK civil servant and international policy advisor, specialising in education and technology. He has also advised foreign Ministers and offices of Prime Ministers on the creation of Delivery Units at the heart of government. From 2018-22, Peter led the 'Secure by Design' initiative across the UK government, which included the creation of the Product Security and Telecommunication Infrastructure legislation, which sought to embed resilience and transparency into IoT products and their associated services. Most recently, Peter led the Global Forum on Digital Security at the OECD, and supported other governments, and G20, as a knowledge partner on security policy issues. Peter is also an experienced public speaker and keynote, having spoken at DEFCON, CES, Singapore Cyber Week, The UN IGF, InfoSec Europe, Cyber UK and many others.

SPEAKERS

Samantha Kight

Head of Industry Security at the GSMA (London)

Samantha Kight is the Head of Industry Security at the GSMA, driving the Security and Fraud direction of the GSMA and working with the industry to execute key initiatives within this space. She is integral in building and maintaining the links between Chief Security Officers across the Mobile Network Operators, providing platforms for Telecommunication security to be discussed and represented globally. Prior to joining the GSMA she worked within a Mobile Network Operator Group and local market function. She has a diverse background having worked across the non-profit, corporate and association sectors and holds a Bachelors and Masters degree from the University of Technology, Sydney.

Thomas Rosteck

Division President Connected Secure Systems at Infineon (Munich)

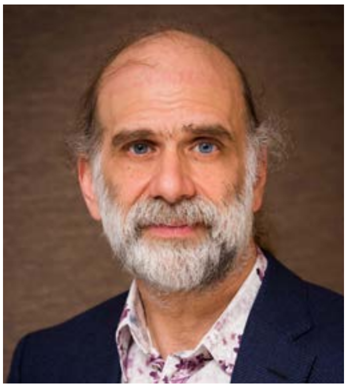
Thomas Rosteck has been Division President Connected Secure Systems at Infineon Technologies AG since 2017. Thomas was born in 1966 in Offenbach am Main, Germany. He studied Business Administration and Computer Science at the Technical University of Darmstadt. He has been with Infineon since 1998 (Siemens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

Kemba Walden

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

Kemba Walden is an American lawyer who serves as the President of the Paladin Global Institute. Walden comes to Paladin after serving as the acting U.S. National Cyber Director in 2023. She joined the Office of the National Cyber Director as its inaugural principal deputy in June 2022. While at the White House, she substantially contributed to the development of and launched the National Cybersecurity Strategy and the corresponding Implementation Plan. Walden also executed the joint OMB/ONCD Spring Guidance to Federal Departments and Agencies on cyber priorities as they develop their fiscal year 2025 budgets. She had a substantial role in developing the National Cybersecurity Workforce and Education Strategy. In addition, Walden lead the U.S. Government in U.S.-Cyber Dialogues with Singapore and Ukraine and was the head of the U.S. Delegation in several international cyber fora, including Cyber UK, Israel Cyber Week, and the OAS Cybersecurity Summit. In 2023, she brought cybersecurity into the global national security conversation at MSC. Walden was previously an Assistant General Counsel in the digital crimes unit at Microsoft where she launched and lead Microsoft's counter ransomware program. Prior to Microsoft, Walden spent a decade in government service at the U.S. DHS most recently at the Cybersecurity and Infrastructure Security Agency where she focused on election security, the financial services sector, and the energy sector.

SPEAKERS



Bruce Schneier

Fellow and Lecturer Harvard Kennedy School (Cambridge, MA)

Bruce Schneier is an internationally renowned security technologist, called a "security guru" by the Economist. He is the New York Times best-selling author of 14 books – including A Hacker's Mind – as well as hundreds of articles, essays, and academic papers. His influential newsletter Crypto-Gram and blog Schneier on Security are read by over 250,000 people. Schneier is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University, a Lecturer in Public Policy at the Harvard Kennedy School, a board member of the Electronic Frontier Foundation and AccessNow, and an advisory board member of EPIC and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.

Jeff Moss

President and Founder of DEF CON (Washington D.C.)

Moss is the founder and creator of both the Black Hat Briefings and DEF CON, two of the most influential information security conferences. DEF CON just had its 31st anniversary. In 2016 Mr. Moss joined Richemont, serving as a Non-Executive Director and a member of the Board's Nominations and Strategic Security Committees. Between April 2011 and December 2013 Mr. Moss was the Chief Security Officer for the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit whose responsibilities include coordinating and ensuring the security, stability and resiliency of the Internet's unique global identifiers as well as maintaining the root zone of the Internet. Prior to creating Black Hat Briefings, Mr. Moss was a director at Secure Computing Corporation where he helped establish their Professional Services Department in the United States, Asia, and Australia. His primary work was security assessments of large multi-national corporations. He has also worked for Ernst & Young, LLP in their Information System Security division. Because of this background Jeff is uniquely qualified to bridge the gap between the underground researcher community and law enforcement, between the worlds of pure research and the responsible application of policy. Mr. Moss is also an angel investor to startups in the security space and was a technical advisor to the TV Series "Mr. Robot" Mr. Moss actively seeks out opportunities to help shape the cybersecurity conversation. Mr. Moss graduated from Gonzaga University with a BA in Criminal Justice.

Jason Ruger

CISO at Lenovo (Chicago)

As Lenovo's CISO, Jason Ruger is responsible for protecting Lenovo customers, employees and shareholders from an ever-increasing array of cyber-attacks. Mr. Ruger is responsible for enabling new products and services that leverage IoT, AI and 5G at the world's largest computer maker. An expert in cyber, cloud and mobile, Mr. Ruger has over 30 years of cyber security and IT experience at Lenovo, Google, Motorola, Apple and Symantec. During his 15+ years as CISO, he successfully led Lenovo, Google and Motorola through some of their largest cyber-attacks in history. While at Google, he led divisional cyber-security for over 25,000 Google employees and created the first smartphone privacy engineering team. While at Motorola, he delivered secure services on 2G, 3G and 4G. Mr. Ruger is a board member and treasurer of the National Cybersecurity Alliance (NCA), a US public private partnership that aims to improve cybersecurity for individuals and organizations. Globally, Mr. Ruger also engages in public / private partnerships as a speaker at the Paris Peace Forum and World Economic Forum. Mr. Ruger holds a Bachelor of Science in Economics from Vanderbilt University and an MBA from Northwestern's Kellogg School of Management. Mr. Ruger serves on the board of a local non-profit, is a founding member of a team that has raised over $1,000,000 to fight cancer and serves meals to the homeless monthly.

SPEAKERS

Koos Lodewijkx

CISO for IBM (Washington D.C.)

Koos Lodewijkx is the Chief Information Security Officer for IBM, responsible for all aspects of IT security ranging from enterprise to product and offering security. Until February 2019, he served as the Chief Technology Officer for IBM Security. Previously, he led IBM's security technical direction as a Chief Technical Officer to the IBM CISO. Koos joined IBM in 2007 with the acquisition of Consul Risk Management, a Netherlands based security software start-up.

Heather Adkins

Vice President Security Engineering at Google (Mountain View)

Heather Adkins is a founding member of the Google Security Team and cybersecurity expert focused on breach recovery, incident response, insider risks and building modern safe computing environments. Heather Adkins is a 21-year Google veteran and founding member of the Google Security Team. As VP, Security Engineering, she has built a global team responsible for maintaining the safety and security of Google's networks, systems and applications. She has an extensive background in practical security, and has worked to build and secure some of the world's largest infrastructure. She is co-author of Building Secure and Reliable Systems (O'Reilly, 2020), co-chairs CISA's Cyber Safety Review Board, and has advised numerous organizations on how to adopt modern defendable architectures.

Paul Vixie

VP and Deputy CISO at AWS (Redwood City)

Paul Vixie is a VP and Distinguished Engineer who joined AWS Security after a 29 year career as the founder and CEO of five startup companies covering the fields of DNS, anti-spam, Internet exchange, Internet carriage and hosting, and Internet security. Vixie earned his Ph.D. in Computer Science from Keio University in 2011 and was inducted into the Internet Hall of Fame in 2014. He is also known as an author of open source software including Cron.

Jonas Andrulis

Founder & CEO of Aleph Alpha (Heidelberg)

Jonas Andrulis is founder and CEO of the German startup Aleph Alpha, with which he has set the German deep-tech funding record since its founding in 2019. He completed his industrial engineering studies at KIT in Karlsruhe, Germany, with a focus on artificial intelligence and modeling. As a serial entrepreneur, prior to Aleph Alpha, he first founded an AI software company for planning and optimization of complex logistics problems, then for human-in-the-loop training and validation of deep learning algorithms for human-machine interactions. As of 2016, he was at Apple leading AI research in the Special Projects Group. With Aleph Alpha, Jonas aims to build an independent European alternative for the next generation of artificial intelligence, following the example of OpenAI and DeepMind.

SPEAKERS

Katie D’Hondt Brooks

Director Global Cybersecurity Policy at Aspen Digital (Washington D.C.)

Katie Brooks serves as Director of Global Cyber Policy Aspen Digital, a program of the Aspen Institute. She leads projects addressing citizen-centric and global cybersecurity challenges. Prior to joining Aspen Digital, Katie consulted government and commercial clients on cybersecurity implementation and strategy. She previously worked at the Partnership for Public Service, where she designed and led programs to recruit entry-level talent to government service. Katie is passionate about creating a more diverse talent pipeline into the cybersecurity field and has presented on the topic at events run by the National Initiative for Cybersecurity Education, the Society of Women Engineers, and the Harvard Women in Public Policy Program.

Lisa O. Monaco

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

Lisa O. Monaco is the 39th Deputy Attorney General of the United States. As Deputy AG, she serves as the Justice Department’s Chief Operating Officer and manages its litigating and policy components, law enforcement agencies, and 93 U.S. Attorneys. Throughout her career, she has worked extensively on national security issues and cyber threats, including in her roles as Counsel to Attorney General Janet Reno; Chief of Staff at the FBI to then-Director Mueller; Assistant Attorney General for National Security, and Assistant to the President for Homeland Security and Counterterrorism Advisor.

John P. Carlin

Partner at Paul Weiss (Washington D.C.)

John P. Carlin is co-chair of Paul Weiss’s Cybersecurity & Data Protection practice and co-chair of the Digital Technology Group. John is 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. John 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.

Cheryl Venable

EVP, Chief of Payment Operations, Federal Reserve Bank of Atlanta (Marietta)

As chief of payments operations, Cheryl manages the teams responsible for Federal Reserve Financial Services (FRFS) payments operations, including FedACH, Checks, and Wholesale (Fedwire Funds, Securities, and the National Settlement Service). In the future, once the FedNowSM Service is launched in 2023, FedNow operations will be included in her area of responsibility. In addition, Cheryl is chair of the Federal Reserve's Business Technology Council (BTC). Prior to her current role, Cheryl was an executive vice president at the Federal Reserve Bank of Atlanta and retail payments product manager for the Retail Payments Office (RPO). In this role, she oversaw all aspects of the Check and ACH payments businesses. Cheryl has spent her entire career with the Fed since joining the St. Louis Bank in 1991 as a management trainee in the accounting and payment system risk department. She joined the Minneapolis Fed in 1996, served as the senior vice president responsible for FedACH operations and automation, led the information technology division, and served on the Management Committee. In 2010 she joined the Atlanta Fed as RPO chief information officer, where she was responsible for Check and FedACH technology and application development, including the successful modernization of the electronic check processing platform.

Cheri F. McGuire

Chief Technology Officer at Swift (Virginia)

Cheri McGuire joined SWIFT in August 2021 as Chief Technology Officer leading the Technology Platform organization of nearly 1,000 team members who deliver resilience, security and trust across the functions of: Production Operations; Platform, Tooling and Enterprise Services; Network, Cloud and Data Center Operations; Cyber and Physical Security; and Business Continuity and Crisis Management. She is a member of the SWIFT Executive Committee and the SWIFT Board Technology and Production Committee. Cheri brings more than 30 years of experience from the financial, IT, consulting and government sectors. Prior to SWIFT, she served as: Managing Director and Group Chief Information Security Officer at Standard Chartered Bank in London; Vice President at Symantec; Director for Critical Infrastructure and Cyber Security at Microsoft; Director of the DHS National Cyber Security Division/US-CERT; Program Manager at Booz Allen Hamilton; and Congressional staffer. She has extensive experience contributing to industry boards and public-private initiatives, currently serving as a non-resident scholar at the Carnegie Endowment for International Peace, on the Monetary Authority of Singapore International Cyber Advisory Panel, and on the AWS CIO Council. She also serves on the Board of Directors for the Cloud Security Alliance and on the World Economic Forum Global Future Council on Cybersecurity. Before SWIFT, she served on the Board of Directors for Entrust Corporation, and the Advisory Boards for Tenable, Security Scorecard, Garrison and X-Analytics Corporations. She also previously served on the Industry Executive Subcommittee of the President’s National Security Telecommunications Advisory Committee, Europol Advisory Group on Financial Services, The George Washington University Center for Cyber and Homeland Security Board, and UK Cyber Defence Alliance Board. From 2010 to 2012, she was Chair of the US IT Sector Coordinating Council. She holds an MBA from The George Washington University and a BA from the University of California at Riverside.

SPEAKERS

Ron Green

Cybersecurity Fellow and Former Chief Security Officer at Mastercard (St. Louis)

Ron Green is a Mastercard Fellow responsible for advocating for strong cybersecurity law and policy with global government and regulatory agencies, deepening public-private partnerships to drive our shared security, and strengthening the cohesion between cyber practices within Mastercard. Previously, Ron served as Mastercard's chief security officer for 10 years from 2014-2024. In this role, he led a global team that ensured the safety and security of the company's network, as well as internal and external products and services. He was responsible for corporate security, security architecture and engineering, cryptographic key management, business continuity, disaster recovery and emergency management. Ron joined Mastercard in 2014 after serving as deputy chief information security officer at Fidelity Information Services (FIS). Prior to this position, he was director, Investigation and Protections Operations at Blackberry. Ron also served as a senior vice president across several areas at Bank of America. He has extensive experience working with international and federal law enforcement agencies both as a special agent in the U.S. Secret Service and as an officer in the U.S. Army. With the Secret Service, Ron worked protection and fraud investigations. He was one of the first agents to receive formal training on seizing and analyzing electronic evidence and worked on a number of international cyber-crime investigations. Ron currently serves as the chair of the Cybersecurity and Infrastructure Security Agency's Cybersecurity Advisory Committee and chair of the U.S. Secret Service's Cyber Investigation Advisory Board. He also served as chair of the Financial Services Sector Coordinating Council (FSSCC) from 2020-2023. He holds a bachelor's degree in mechanical engineering from the United States Military Academy at West Point, is a graduate of the FBI's Domestic Security Executive Academy and holds a graduate certification in Information Assurance from George Washington University.

Rafael Garcia Oliva

Deputy Director General in the Directorate General Information Systems at ECB (Frankfurt)

Rafael Garcia Oliva has been ECB Deputy Director General in the Directorate General Information Systems since April 2023, effectively acting as head of the ECB's IT directorate. He held numerous managerial positions in the ECB's IT directorate after initially joining the ECB as an IT expert in 2000. Prior to working at the ECB, he was responsible for the network and communications of a NATO Agency and an engineer officer in the Spanish Air Force. Rafael is a Telecommunications Engineer and holds a Master in Applied Science on International Finance and a Master in Business Administration from the Open University of the UK.

Sergej Epp

Chief Security Officer EMEA Central at Palo Alto Networks (Frankfurt)

Sergej Epp is tech-savvy Chief Security Officer at Palo Alto Networks in EMEA Central. In this role, he develops cybersecurity strategy, overseeing cybersecurity operations and threat intelligence and is acting as a trusted advisor to strategic customers across the region. Prior to joining Palo Alto Networks, he spent nine years in a variety of cybersecurity roles at Deutsche Bank, where he built and led cyber defense & investigations teams focusing on cybercrime, malware, supply chain, insider threat, and fraud. Sergej studied at the Frankfurt School of Finance and Management and University of New Zealand. He participates regularly as a speaker at conferences, acts as executive lecturer for Fortune500 management boards at Frankfurt School and is an advisor to venture capital funds and high-tech start-ups.

SPEAKERS

Wolfram Seidemann

CEO at G+D Currency Technology (Munich)

Wolfram Seidemann has been Chief Executive Officer of Giesecke+Devrient Currency Technology since July 2017. As an Executive Committee member of the Giesecke+Devrient Group, he holds the responsibility for overseeing the Public Currency activities, which encompasses the Physical Banknote business as well as the Central Bank Digital Currency (CBDC) business of Giesecke+Devrient advance52. Prior to this, Wolfram held a number of executive management positions as Group Executive Banknote at Giesecke+Devrient, Chairman of the Management Board of Papierfabrik Louisenthal, and Head of Sales and Marketing of Banknote Processing Systems worldwide.Wolfram joined Giesecke+Devrient as Head of International Research and Development Chipcard in 1999 and has served since in various management positions in Munich, Singapore, Taiwan, and New Delhi. His background is in Electrical Engineering and Business Administration. He holds a PhD in Innovation Management from the Technical University of Munich, where he began his career as Head of R&D and Innovation Management of the Economics Department, later working as an industry consultant in the field. Since 2018, Wolfram has been serving as a Board Member of the International Currency Association (ICA), an organization dedicated to promoting and representing the perspectives of the currency industry, of which he held the position of Chairman from 2018 to 2022.

Akihiro Wada

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

Mr Wada assumed the chairpersonship of the Working Group on Cyber-Security Enhancement, Committee on Cyber Security, Keidanren in April 2022. At All Nippon Airways, Mr Wada is Senior Director responsible for information security & IT architecture strategy. Through his career, he retains large-scale project management skills as well as practical knowledge on the Information Security Management System and the Personal Information Protection Law. Mr Wada’s public activities include postings at various government agencies as well as the Cyber Risk Intelligence Centre – Cross Sectors Forum, where he is currently vice chair, as well as Chief Director at Transportation ISAC Japan. Mr Wada holds a BSc (Science) from Kyushu University.

Emily Goldman

U.S. Cyber Command (Washington D.C.)

Dr. Emily Goldman serves as a strategist at U.S. Cyber Command and a thought leader on cyber policy. She was cyber advisor to the Director of Policy Planning at the Department of State, 2018-19. From 2014 to 2018 she directed the U.S. Cyber Command / National Security Agency Combined Action Group, reporting to a four-star commander and leading a team that wrote the 2018 U.S. Cyber Command vision, Achieve and Maintain Cyberspace Superiority. She has also worked as a strategic communications advisor for U.S. Central Command and for the Coordinator for Counterterrorism at the State Department. She holds a doctorate in Political Science from Stanford University and was a Professor of Political Science at the University of California, Davis, for two decades. Dr. Goldman's most recent book, Cyber Persistence Theory: Redefining National Security in Cyberspace, with Michael Fischerkeller and Richard Harknett, was published by Oxford University Press in 2022.

SPEAKERS

Manfred Boudreaux-Dehmer

NATO Chief Information Officer (Brussels)

Dr. Manfred Boudreaux-Dehmer is the inaugural Chief Information Officer (CIO) of the North Atlantic Treaty Organization (NATO). He commenced his position at NATO Headquarters in Brussels, Belgium on September 1, 2021. His principal responsibility is to realize the Allies' vision for Information and Communications Technology (ICT) in support of NATO's purpose to guarantee freedom and security for its 31 member nations. Under the mandate of the North Atlantic Council, and under the delegated authority of the NATO Secretary General, he is tasked with facilitating ICT coherence across NATO's 50+ civil and military bodies with 25,000 users. He also performs the Chief Information Security Officer (CISO) function as the Single Point of Authority for cybersecurity. From 2010 until 2021, Dr. Boudreaux-Dehmer directed all global computing and information technology systems for Sierra Wireless in Vancouver, Canada. The company provides Internet of Things (IoT) solutions that empower businesses to thrive in the interconnected global economy. Prior to assuming this role, he spent eight years at Hewlett-Packard (HP) IT in Business Intelligence and Strategy & Planning leadership roles. From 1993 to 2002, he oversaw Supply Chain systems at Compaq's Latin America Division in Houston, Texas and São Paulo, Brazil. Prior to that, he supported material planning processes at Compaq's European Headquarters in Munich, Germany and Gorinchem, The Netherlands. Dr. Boudreaux-Dehmer has an MBA from Duke University, Durham, North Carolina. He also holds a Master of Science (MSc) in Business and Management Research and a Doctorate in Business Administration from the University of Reading, UK.

Pekka Jokinen

Director at National Cyber Security Center Finland (Helsinki)

Pekka Jokinen works as a director at National Cyber Security Center Finland. His main responsibility is lead the incident handling in wide scope, lead the preparedness and readiness of the center as well as all cooperation internally in Finland and internationally. Mr Jokinen has 20 years of background from the Finnish Defence Forces. Jokinen is a general staff officer and has served multiple positions in Armoured Brigade, Karelia Brigade and Defence Staff. His last appointment at Defence Staff was to be responsible of the strategic planning at cyber defence.

Michael Rogers

Admiral (ret.) U.S. Navy (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.

Alexander Klimburg

Senior Fellow at The Hague Center for Strategic Studies (The Hague)

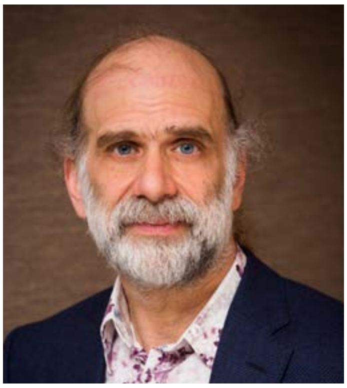
Alexander Klimburg is a Senior Fellow at The Hague Center for Strategic Studies (The Hague), the Institute for Advanced Studies (Vienna), as well as a Senior Associate (non-resident) at the Center for Strategic and International Studies (Washington DC). Previously he served as the Head of the Center for Cybersecurity at the World Economic Forum, and as the director of the Global Commission on the Stability of Cyberspace. He also held appointments as a fellow and associate of the Harvard Kennedy School's Belfer Center as well as the Berkman Klein Center, and was a non-resident senior fellow at the Atlantic Council. Dr. Klimburg has given testimony to parliaments and advised a number of governments, businesses and international organizations on cybersecurity strategies, international norms of behavior in cyberspace and cyber conflict, cybercrime, and cyber espionage; critical infrastructure protection; and Internet governance. He has participated in international and intergovernmental discussions, inter alia, within the UN, EU, OSCE, and G20.

David Lashway

Partner at Sidley (Washington D.C.)

David Lashway is co-chair of Sidley Austin's Tier 1 ranked Global Privacy and Cybersecurity Practice and a member of the firm's top ranked Global Crisis Management and Strategic Response team. Mr. Lashway is based in Washington, DC, and he is acknowledged as one of the leading lawyers for crisis management, cybersecurity, data security incidents, misinformation and disinformation, trade secret theft, espionage, 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 responses to operationally impactful malware for a number of Fortune 500 entities. He routinely leads responses to ransomware-related matters. He also has served as lead counsel on matters for organizations facing difficult regulatory, legislative, and public policy issues across a range of industry sectors and subjects. Mr. Lashway is a frequent speaker on cybersecurity and national security matters and is an expert in the law of cyber armed conflict.

AI Needs to Be Both Trusted and Trustworthy



Bruce Schneier

Fellow and Lecturer
Harvard Kennedy School (Cambridge, MA)

In 2016, I wrote about an Internet that affected the world in a direct, physical manner. It was connected to your smartphone. It had sensors like cameras and thermostats. It had actuators: Drones, autonomous cars. And it had smarts in the middle, using sensor data to figure out what to do and then actually do it. This was the Internet of Things (IoT).

The classical definition of a robot is something that senses, thinks, and acts – that's today's Internet. We've been building a world-sized robot without even realizing it. In 2023, we upgraded the "thinking" part with large-language models (LLMs) like GPT. ChatGPT both surprised and amazed the world with its ability to understand human language and generate credible, on-topic, humanlike responses. But what these are really good at is interacting with systems formerly designed for humans. Their accuracy will get better, and they will be used to replace actual humans. In 2024, we're going to start connecting those LLMs and other AI systems to both sensors and actuators. In other words, they will be connected to the larger world, through APIs. They will receive direct inputs from our environment, in all the forms I thought about in 2016. And they will increasingly control our environment, through IoT devices and beyond.

It will start small: Summarizing emails and writing limited responses. Arguing with customer service – on chat – for service changes and refunds. Making travel reservations. But these AIs will interact with the physical world as well, first controlling robots and then having those robots as part of them. Your AI-driven thermostat will turn the heat and air conditioning on based also on who's in what room, their preferences, and where they are likely to go next. It will negotiate with the power company for the cheapest rates by scheduling usage of high-energy appliances or car recharging. This is the easy stuff. The real changes will happen when these AIs group together in a larger intelligence: A vast network of power generation and power consumption with each building just a node, like an ant colony or a human army.

Future industrial-control systems will include traditional factory robots, as well as AI systems to schedule their operation. It will automatically order supplies, as well as coordinate final product shipping. The AI will manage its own finances, interacting with other systems in the banking world. It will call on humans as needed: to repair individual subsystems or to do things too specialized for the robots. Consider driverless cars. Individual vehicles have sensors, of course, but they also make use of sensors embedded in the roads and on poles. The real processing is done in the cloud, by a centralized system that is piloting all the vehicles. This allows individual cars to coordinate their movement for more efficiency: braking in synchronization, for example. These are robots, but not the sort familiar from movies and television. We think of robots as discrete metal objects, with sensors and actuators on their surface, and processing logic inside. But our new robots are different. Their sensors and actuators are distributed in the environment. Their processing is somewhere else. They're a network of individual units that become a robot only in aggregate.

This turns our notion of security on its head. If massive, decentralized AIs run everything, then who controls those AIs matters a lot. It's as if all the executive assistants or lawyers in an industry worked for the same agency. An AI that is both trusted and trustworthy will become a critical requirement. This future requires us to see ourselves less as individuals, and more as parts of larger systems. It's AI as nature, as Gaia – everything as one system. It's a future more aligned with the Buddhist philosophy of interconnectedness than Western ideas of individuality. (And also with science-fiction dystopias, like Skynet from the Terminator movies.) It will require a rethinking of much of our assumptions about governance and economy. That's not going to happen soon, but in 2024 we will see the first steps along that path.

This essay previously appeared in Wired.

DISARM: An open framework for those cooperating in the fight against disinformation

Malicious actors are using disinformation as a tool to undermine democracy and attack crucial faculties for decision-making from the corporate to the political. What is needed is an all-of-society response, which is hard to coordinate. To enable this, there is DISARM (Disinformation Analysis and Risk Management), an open-source language on disinformation tactics. DISARM has now become the de-facto global standard for exchanging data and analysis on disinformation behaviours. The Framework has been developed drawing on global cybersecurity best practices. It is used to help communicators, from whichever discipline or sector, to gain a clear shared understanding of disinformation incidents and to immediately identify defensive and mitigation actions that are available to them. The framework was constructed based on both historical and hypothetical tactics and techniques employed by manipulators and responses employed by defenders, to provide a comprehensive set of known and anticipated manipulator behaviours and defender actions.

The tangible impact of DISARM has been seen through its successful deployment across a number of global agencies and country teams. These include defending democracy, supporting pandemic communication and addressing other disinformation campaigns around the world, by institutions including the European Union, United Nations and NATO. DISARM has been adopted as part of the formal system for information exchange between the EU and US government. It has been taken up by the major tech platforms, with Meta, Google, and Microsoft now using this approach for common reporting on disinformation tactics. The framework has helped establish new institutions, including the Cognitive Security ISAO, the Computer Incident Response Center Luxembourg and OpenFacto's analysis programme, and has been used in the training of journalists in Kenya and Nigeria. DISARM was employed within the World Health Organization's operations, countering anti-vaccination campaigns across Europe. The use of framework methodology enabled the coordination of activities across teams and geographies, and also – critically – across multiple languages, eliminating the need to translate text by matching actions to numbered tactics, techniques and procedures within the framework.

The DISARM Framework is maintained by the DISARM Foundation, with the support of the nonprofit Alliance4Europe.

Contact: Benjamin Zeeb, Head of Partnerships.
Email: benjamin.zeeb@alliance4europe.eu

Alliance 4Europe DISARM FOUNDATION

Why Data, AI, and Regulations Top the Threat List for 2024

Steve Durbin

Chief Executive of Information Security Forum ISF

"Security leaders must navigate turbulent waters of data deluge, AI ethics, and evolving regulations to keep businesses afloat."

The new year finds us confronted by a landscape characterized by political uncertainty, social fragmentation, and escalating geopolitical tensions. Amidst this turbulent macro-economic backdrop, it is crucial that security leaders strategically prepare for the forthcoming challenges. Let's explore the three main security challenges businesses will face in 2024:

1. Data

Modern businesses generate and manage vast volumes of data daily. Since data is central to decision-making and competitive advantage, its sudden disruption or unavailability can lead to severe repercussions for the business. As security teams, some of the essential questions we ought to be asking include: How do we manage and safeguard aspects like confidentiality, integrity, and availability of data? What strategies can we employ to protect our data against cyber threats and misuse? How do we address the security challenges that emerge with expanding data repositories? How do we differentiate between valuable data and redundant information?

Furthermore, there's often a misalignment in how data is structured versus the business framework. Consequently, security teams may need to engage in discussions with business units to clarify issues such as how we are applying our data. With whom is this data being shared? Who holds accountability for it? Who is responsible for making decisions regarding data security, the information security team, the chief executive, the board, or a combined effort?

2. Artificial Intelligence

Although AI technologies aren't new, the recent widespread adoption of AI has introduced a myriad of business and security challenges for organizations. Key questions to consider include: How do we monitor AI usage within the organization? How do we regulate the data shared with AI systems by employees? How do we ensure ongoing compliance with ethical standards and legal requirements?

Data is the cornerstone of AI. How do we provide sufficient data for AI systems while ensuring this data is secure, ethical, and transparent? How do we safeguard AI data and algorithms from manipulation by threat actors? Security teams need to be vigilant about all AI-related risks, including ethical concerns. Despite these challenges, AI offers significant opportunity for companies aiming to evolve and enhance their business models. In 2024, corporate boards will likely assume a central role in overseeing AI's secure deployment across the organization. This scenario presents a prime opportunity for security teams to align closely with business objectives, be at the forefront of the AI revolution, and actively participate in key business decisions alongside management teams.

3. Regulations

Security is rapidly evolving, and so are regulations governing it. Over the next 12 months, several regulations will either be introduced, updated, or reviewed. For example, the updated NIST standard (NIST 2) will come into effect in 2024; GDPR may announce stringent reinforcements in 2024; the Digital Operational Resilience Act (DORA) will apply to financial entities across the EU; the EU AI Act may also get established or agreed upon.

Given these developments, organizations must develop a comprehensive understanding of the regulations in the jurisdictions where they operate. This knowledge is crucial for building the necessary processes and frameworks proactively, as once these regulations are enforced, adjusting to them retroactively will be challenging. Hence, staying ahead of these regulations in 2024 is imperative, as non-compliance could lead to severe legal, financial, and reputational consequences.

How Can Cybersec Leaders Address These Securitry Challenges?

Below are four risk management initiatives that cybersecurity leaders can integrate into their 2024 cybersecurity planning:

1. Communicate Issues in Business Terms

It's essential for cybersecurity leaders to present issues in a manner that resonates with business leaders. CEOs typically prefer to avoid technicalities. Their concern is how technology will impact the business and whether it aligns with overall objectives. Will it meet stakeholder expectations? What are the risks in terms of financial, operational, and economic factors, beyond technical aspects?

2. Establish Clear Risk Tolerance Levels

For security leaders working with management teams, it’s crucial to define the company’s risk tolerance concerning cyber loss, akin to other risk types. For instance, what is the risk tolerance for employing generative AI? Who is responsible for making this decision? What regulations are relevant, and how will this affect the information we disclose?

3. Implement a Robust and Practiced Response Plan

Executive teams and boardrooms seek assurance. They require confidence that the organization is prepared for unexpected crises, ensuring there is comprehensive situational awareness across the organization, and confirmation that vigilant monitoring of activities is ongoing. They need reassurance that fundamental cyber protection measures are implemented and that a thoroughly documented and regularly rehearsed business continuity and response plan is ready to be activated in the event of a security incident.

4. Build Awareness, Foster Accountability in the Workforce and Supply Chain

The nature of work has transformed significantly in recent years, necessitating updates in security policies and procedures to reflect these changes. Organizations must explicitly outline accountability for data collection and usage, engage in collaborative and transparent interactions with stakeholders, and ensure everyone understands their role in safeguarding the business. Likewise, it's crucial to extend the same security principles and procedures to third parties and supply chain partners that handle data on behalf of the parent organization. To summarize, we're facing three key areas that will continue to grow in complexity and challenge: data, AI, and regulation. There's an increasing expectation for closer engagement between security teams and business operations, coupled with board directors' growing concerns about their personal liability. If security leaders concentrate on these threat management initiatives, they can significantly help mitigate risk and contribute to building a resilient organization into the future.

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.

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

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 2026

The era of entangled risks

1 /

Technology Accelerates

Access to innovation:
Easy/Hard

Nature of innovation:
Disruptive/Predicable

1.1 Riding the wave
1.2 Smooth sailing
1.3 Hitting the wall
1.4 Stumbling and falling

2 /

Society Divides

Source of information:
Facts/Opinions

Identity of group:
Community/National

2.1 Motivated workforce
2.2 Splintered globe
2.3 The filter bubble
2.4 Ideological chess game

3 /

Climate Deteriorates

Speed of change:
Steady/Sudden

Pressure to respond:
High/Low

3.1 Zero motivation
3.2 Relief at last
3.3 Disaster incoming
3.4 Final chance

INFORMATION SECURITY FORUM
Better Cybersecurity

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.

Generative AI Risk Factors on 2024 Elections

Vivien Schiller

VP and Executive Director, Aspen Digital (Washington D.C.)

Josh Lawson

Director, AI and Democracy, Aspen Digital (Washington D.C.)

More than 2 billion people are eligible to participate in major global elections that will occur throughout 2024. With anti-democratic movements deepening their grip, the stakes could not be higher.

Trust in democratic institutions and facts themselves faced headwinds long before the public gained access to new generative AI tools. While the underlying technology is not entirely new, OpenAI's public launch of ChatGPT in November 2022 unleashed a mix of euphoria and hand wringing from a public coming to terms with such capable tools.

There is no firm consensus whether generative AI threats in the civic context represent a difference in degree or a difference in kind. Some suggest wide availability of fast-evolving AI tools simply exacerbate familiar misinformation challenges from familiar bad actors. But others cite the exponential rate of technological improvements and the promise of ever-greater speed, scale, and sophistication as reason enough to expect and to counter a dramatic erosion in trust across democratic institutions, including elections.

Our research at Aspen Digital yielded seven risk factors:

1. **Siloed Expertise:**
   Elections officials are not up to date on AI capabilities and unlikely to know where they can turn for help, we found in conversations. The AI labs and some tech companies are not attuned to the challenges elections officials face. "There's very little understanding about how democracy works," said an expert who engages regularly with AI labs and tech companies. Dots aren't being connected amongst AI experts; mis- and dis-information specialists; elections officials; and policymakers. This is certainly true in the US, and we expect even greater disparities globally.

2. **Public Readiness:**
   Experts doubt the public will be resilient in the face of AI tools, which some expect to "flood the zone" with believable falsehoods during crises. Even if the public infrequently encounters AI-generated content, a surge in press coverage around AI capabilities might be enough to trigger public reactions that affect civic behavior–including an erosion in public trust overall. As a result, people may revert to sources they already trust regardless of veracity, or reject factuality in general, a phenomenon known as the "liar's dividend." These outcomes do not require personal exposure to fake content but may occur simply because the public is aware that content could be fake.

3. **Inadequate Platform Readiness:**
   Over the last two years, major platforms have cut staff across integrity operations, and offered less transparency to media and researchers. Generative AI is likely to pressure already-taxed platform resources, experts said. The capacity to generate volumes of content at speed may overwhelm fact-checking efforts, even as the ability to produce unlimited variations of the same underlying claim might avoid detection by integrity tools built to prioritize the virality of a particular post (not a general claim).

4. **Slow Moving regulation:**
   The EU recently enacted regulations to hold platforms accountable for "harmful content" (or face a financial penalty), and they are acting quickly to create an "AI Act" that could have broad implications worldwide. The AI Act, along with a joint effort between the US and the EU to create a transatlantic AI Code of Conduct are under consideration, but would take so long to be adopted that they will not impact the 2024 election cycle. In the US, many efforts are underway at the local and state levels, but federal policy is not expected before November elections.

5. **Increasing Quality AI-Generated Media:**
   As AI-generated content has increased in quality, visual instinct alone is increasingly unreliable. Consequently, policymakers and others have shifted their mitigation efforts to overt labeling of AI generated content, digital signatures–so-called "watermarking" technologies that are still in their infancy.

6. **Scaled Distribution at High-Speed:**
   Until recently, substantial resources were needed to draft convincing misinformation or to effectively alter audio/visual content. Technical expertise and language requirements prevented some bad actors from creating and distributing large volumes of content. AI dramatically lowers these barriers and allows people to generate high-quality content that may restate the same false claim in many different ways or depict fake events from multiple camera angles, for example.

7. **Message Targeting & Hyperlocal Misinformation:**
   Generative AI may supercharge targeting capabilities by allowing creators to dramatically scale so-called "A/B testing," producing so many variations of content that targeting models grow exponentially robust as users engage with particular messages. Some believe these capabilities will result in such granular targeting that messages will essentially be honed to particular psychological profiles–what some have called "superhuman persuasion."

   AI may also generate compelling content that appears credible simply because it references highly localized information – "hyperlocal misinformation"– such as the name of the school where a precinct is located or the names of streets and neighborhoods. Some are concerned that people will use AI to create hyperlocal misinformation about conditions at critical polling locations or safety in certain locations on Election Day. The risk is particularly acute given improvements across language groups.

8. **Automated Harassment:**
   Bad actors may create harassing content targeting elections administrators, activists, journalists, and other civic leaders and topics for a number of reasons: to intimidate, to reduce the algorithmic distribution of a post by adding large volumes of toxic comments, or to sway opinion during a crisis by appropriating particular hashtags.

9. **Cybersecurity of Elections Infrastructure:**
   Experts we spoke with raised concern that generative AI is a boon for social engineering scams, including phishing attacks, raising concerns that AI-enabled audio impersonation could spoof official communications from superiors to poll workers AI capabilities are also expected to enhance malware as fast-evolving code generation and analysis features are increasingly integrated into AI tools.

These developments underscore the urgent need for coordination, prioritization, and accountability across all sectors with stakes in a shared democratic future. The coming months will require policymakers, tech companies, and civil society to take responsible action in the face of evolving social and technological shifts in a critical election year.

Vivian Schiller is VP and Executive Director, Aspen Digital

Josh Lawson is Director, AI and Democracy, Aspen Digital

Aspen Digital is a program of the Aspen Institute

ASPEN DIGITAL
aspen institute

Charter of Trust

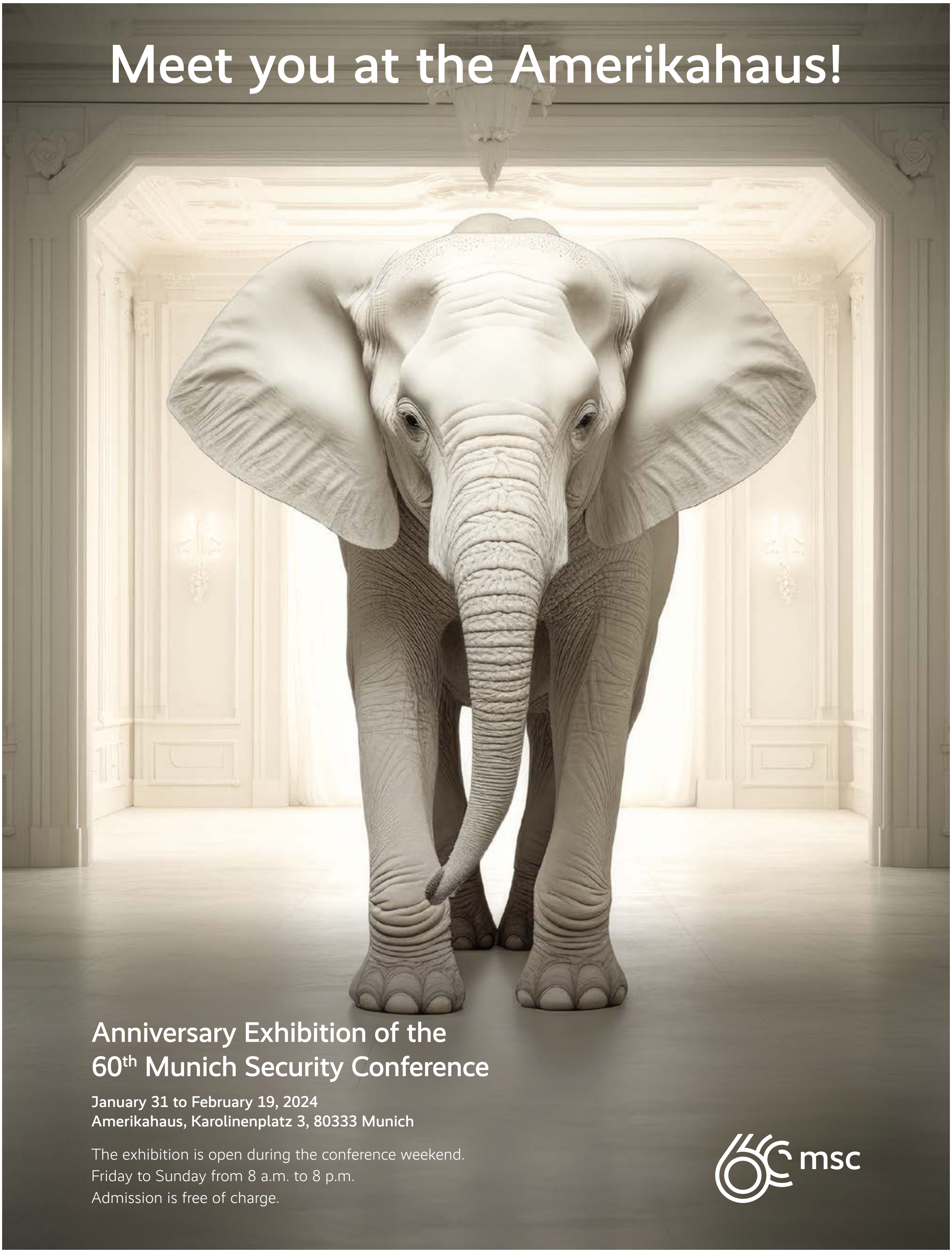
For a secure digital world

Rarely before has the ability to innovate determined a country's position in geopolitical power play as today. Quantum computing and AI are emerging as disruptive forces that have the potential to create spheres of technological influence. As a result, technological leadership and industrial policies have become critical factors in a nation's geopolitical strategy. Simultaneously, hybrid threats have risen to an integral part of modern warfare. Unconventional hybrid methods, encompassing ransomware attacks, cyber espionage, or disinformation campaigns, are adeptly veiled in plausible deniability, thereby complicating detection and attribution. The potential damage is severe, underscoring the need for robust cybersecurity at both the societal and national levels as a pillar of national defence. This requires a collective and coordinated effort involving governments, businesses, and technology leaders.

The Charter of Trust, launched in 2018 at the Munich Security Conference, contributes to the development of effective, harmonized cybersecurity policies that strengthen global cybersecurity posture and provides hands on expertise based on best practices for topics including AI, security by default, supply chain security, and education.

We can shape Cybersecurity - together.
Find out more www.charteroftrust.com

aes Allianz Atos BOSCH
DELL Technologies IBM infineon Microsoft
MITSUBISHI HEAVY INDUSTRIES msc NXP SIEMENS
TotalEnergies TÜV SÜD



Anniversary Exhibition of the 60th Munich Security Conference

January 31 to February 19, 2024
Amerikahaus, Karolinenplatz 3, 80333 Munich

The exhibition is open during the conference weekend.
Friday to Sunday from 8 a.m. to 8 p.m.
Admission is free of charge.

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, Suntka von Halen, David Lashway, Geoff Brown, Christopher Ahlberg, Wolfram Seidemann, Michael Hochholzer, Thorsten Delbrouck, Valentin Weber, Wolfgang Baare-Schmidt, Tobias Kiesling, Thomas Tarantino, Stefan Lankes, June Chambers, Jens Redmer, Martin Loss, Koh Nakaji, Shinichi Yokohama, Franziska Armbruster, Alexander Wieser, Arthur de Liedekerke, Ieva Ilves, Vivian Schiller, Jeff Greene, Katharine Brooks, Stormy Mildner, Molly Hall, Graham Holliday, Benno Müchler, Kushal Prakash, Ingrid Dickinson, Jordana Siegel, Timo Blenk, Silke Huber-Voigt, Marina Hoffmann, Marina Geigenberger, Christine Schmerber, Sergej Epp, Kai Hermsen, Kathrin Wagenhuber, Paul Desprez, Robert Kosla, Phlip Stupak, Janet Bosshammer, Werner Theiner, Stefan Jost-Dummer, Bernhard Rohleder, Kerstin Petretto

This conference was organised by:

Peter Moehring
Managing Director Security Network Munich

Lorenz Hoeppl
Security Network Munich

Charlotte Kobel
Security Network Munich

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

Marc Raimondi
Chief of Staff at Silverado Policy Accelerator

John Mengers
Founder and Executive Director of C-Suite Advisors

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.