



SECURITY NETWORK MUNICH
PRESENTS

MCSC

MUNICH CYBER SECURITY
CONFERENCE **2020**

Fail safe – Act brave: Building a Secure and Resilient Digital Society

Hotel Bayerischer Hof
Munich, February 13, 2020
2:00 – 7:30 pm

Followed by Reception and Networking Party

In Cooperation with:

Bavarian Ministry of Economic Affairs,
Regional Development and Energy



Munich Security
Conference **MSC**
Münchner Sicherheitskonferenz

Supported by:

AIRBUS

GD Giesecke+Devrient
Creating Confidence



secunet



sic[!]sec



Google



SIEMENS
Ingenuity for life

CMD^CTRL
Munich 2020

REPLY
SPIKE

Media partners:



The Security Times

Ladies and Gentlemen,

It gives me great pleasure to welcome you all to the 6th edition of the Munich Cyber Security Conference.

Over the twelve months since our last gathering, we have witnessed many important developments with regard to information and cyber security, the topic of 5G security being amongst the most consequential.

This year's conference programme will reflect on these issues and hopefully inspire discussion among you, our distinguished guests.

Today's agenda include Digital Sovereignty (or Strategic Autonomy to use the preferred term in military circles), the protection of our critical infrastructure, and the challenge of securing the Internet of Things as hyper-connected systems increasingly affect our physical world.

There is no doubt that a lack of widespread technical knowledge, insufficient trust, transparency and coordination negatively affects policymaking and regulation efforts, weakening the ability to achieve satisfactory levels of cyber resilience.

As EU Commissioner Margrethe Vestager recently pointed out "Cybersecurity is only as good as the weakest link". To improve these links, she encouraged a shared security culture and enhanced cooperation among partners and Member States – both at the political level and, more importantly, at the industry level.

The Munich Cyber Security Conference was started six years ago to encourage dialogue and improve cooperation among decision makers from private and public sectors across the world.

I am delighted that you are all here today to continue this tradition and I wish you all a thought-provoking afternoon of open and constructive discussion.

Thank you.



Ralf Wintergerst

HOST: SECURITY NETWORK MUNICH



Ralf Wintergerst

Chairman Security Network Munich & Group CEO
Giesecke+Devrient (Munich)

As CEO of Giesecke+Devrient (G+D) Ralf Wintergerst is managing one of the world's leading security technology companies. He began his career in 1998 as Director of International Subsidiaries in the Cards and Services business. Between 1999 and 2005 he held various management positions in the division Currency Management Solutions, ultimately heading it from 2006 on. He has been a member of the Management Board since 2013. In 2016, he was appointed Chairman of the Management Board. Furthermore to his role at G+D, Wintergerst is Chairman of the Supervisory Board of secunet Security Networks AG. In addition, he holds various positions related to IT security issues, including member of the advisory board of the Cyber Defense research institute of the Bundeswehr University in Munich and co-chair of the Digital Summit Platform "Security, Protection and Trust" of the Federal Ministry of the Interior. Since mid-2019, he took over as chair of the North Africa Middle East Initiative of German Business (NMI) and has also become a member of the Executive Committee of Germany's digital association, Bitkom.

Dear participants,

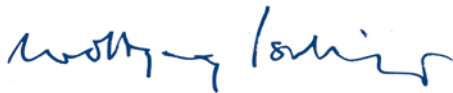
I am delighted that the eve of the 56th Munich Security Conference serves as an occasion for so many distinguished experts in this field to assemble at the Munich Cyber Security Conference MCSC again this year.

The ever-increasing significance of cyber security has been reflected in a growing range of activities on the MSC's calendar – both at our main conference and beyond. Over the past years, our Cyber Security Summits have convened at hubs of digital innovation around the world. True to our conviction that cyber security is an issue to be addressed at the highest levels, both in the private sector and in government, the Summits have brought together senior decision-makers with experts from academia and civil society.

Our partnership with the MCSC is an important part of our commitment to advancing the debate on cyber issues, and we look forward to a continued cooperation to enable more of these constructive and thought-provoking discussions.

I now wish you a fruitful exchange here in Munich, and encourage you to challenge each other and embrace new perspectives.

Sincerely yours,



Wolfgang Ischinger

Chairman of the Munich Security Conference

Munich Security
Conference **MSC**
Münchner Sicherheitskonferenz

Honored guests,

Cyber security is of extraordinary economic importance and a central focus of Bavaria's High-Tech Agenda. Cyber crime inflicts an annual loss of more than USD 660 million on businesses worldwide, with that figure rising continuously.

While Bavaria is already a leader in cyber security today, and we will continue to work on advancing that status in all of its aspects. One example is the Cyber Security Platform at Center Digitisation Bavaria which is closely interlinked with the networking initiatives put forward by Bavaria's IT security companies and users of these technologies.

There is also the Fraunhofer Institute for Applied and Integrated Security (AISEC) in Garching, which we have been supporting since 2012. Under our High-Tech Agenda, we will be teaming up with the Cyber Security Learning Lab at the OTH Amberg-Weiden Technical University of Applied Sciences. The goal is not only to protect the economy against security risks, but also to raise awareness for the current challenges associated with cyber security.

Thank you for being our guests today. I wish you a stimulating and successful conference.



His Excellency Hubert Aiwanger

Bavarian Minister of Economic Affairs, Regional Development and Energy, Deputy Minister President of Bavaria

Bavarian Ministry of Economic Affairs,
Regional Development and Energy



**Ambassador
Wolfgang Ischinger**



Hubert Aiwanger

IMPRINT

Publisher:
Security Network Munich

Layout:
Zeilbeck Design Company

© Security Network Munich, 2020
All rights reserved

SIXTH INTERNATIONAL MUNICH CYBER SECURITY CONFERENCE (MCSC) 2020

Fail safe – Act brave: Building a Secure and Resilient Digital Society

2:00–2:30 pm	<p>Welcome</p> <p>Opening Address</p> <p>Keynote</p>	<p>Ralf Wintergerst Chairman Security Network Munich & Group CEO Giesecke+Devrient (Munich)</p> <p>His Excellency Margaritis Schinas Vice-President of European Commission in Charge of Security Union Europe (Brussels)</p> <p>His Excellency José Angel Gurría Secretary-General of OECD (Paris)</p>
2:30–2:50 pm	<p>Impulse Speech</p> <p>Impulse Speech</p>	<p>Reinhard Ploss CEO Infineon (Munich)</p> <p>Kristie Canegallo VP of Trust & Safety Google (Mountain View, CA.)</p>
2:50–3:40 pm	<p>First Panel Mission Critical: Effectively Protecting Critical Infrastructure</p> <p>Moderator: Kiersten E. Todt Cyber Readiness Institute CRI</p>	<p>Christopher C. Krebs Director Cybersecurity & Infrastructure Security Agency CISA (Arlington, VA)</p> <p>Scott Jones Head-designate Canadian Centre for Cyber Security (Ottawa)</p> <p>Patricia Zorko Deputy National Coordinator for Security and Counterterrorism NCTV, Ministry of Justice and Security (The Hague)</p> <p>Ciaran Martin CEO National Cyber Security Centre (London)</p> <p>Michael Punke VP Global Public Policy Amazon Web Services (U.S.A.)</p>
3:40–4:10 pm	<p>Break</p>	
4:10–4:25 pm	<p>Keynote</p> <p>Impulse Speech</p>	<p>Seiji Ninomiya Director-General for Global Cybersecurity Policy, Ministry of Internal Affairs and Communications MIC (Tokyo)</p> <p>Shinichi Yokohama CISO NTT Group (Tokyo)</p>

4:25–5:15 pm	Second Panel Digital Sovereignty In The Geo-Politics of Cyber Security – A Myth?	Arne Schönbohm President of Federal Office for Information Security BSI (Bonn) Josh Cowls Research Associate in Data Ethics, Alan Turing Institute (Oxford) Juhan Lepassaar Executive Director of EU Agency for Cybersecurity ENISA (Crete) Markus Braendle Head of Airbus CyberSecurity (Munich) Sandra Joyce SVP Global Intelligence FireEye (U.S.A.)
5:15–5:45 pm	Break	
5:45–6:10 pm	Spot on Moderator: Gregor Peter Schmitz Augsburger Allgemeine	Alex Stamos Director Stanford Internet Observatory, Stanford University (U.S.A.) Jeff Moss Founder of DEF CON and Black Hat Briefings (U.S.A.) Sergej Epp CSO Palo Alto Networks (Munich)
6:10–6:30 pm	Government Perspective Global View	Joachim Herrmann State Minister of the Interior, Government of Bavaria (Munich) Steve Durbin MD of Information Security Forum ISF (London)
6:30–7:20 pm	Third Panel Known Unknowns: Securing The Internet (of Things) With Unsecure Parts Moderator: Tom Koehler connecting trust	Yigal Unna Director General of Israel National Cyber Directorate INCD (Israel) Donald D. Parker VP Product Assurance and Security Intel (Santa Clara, CA.) Natalia Oropeza Chief Cybersecurity Officer Siemens (Munich) Axel Deininger CEO Secunet (Munich) Claudia Eckert MD of Fraunhofer Institute AISEC (Munich)
7:20–7:30 pm	Greeting	Roland Weigert Vice Minister, Government of Bavaria (Munich)
7:30–9:30 pm	Reception and Networking Party	

EDITORIAL



Steve Durbin

Managing Director of the Information Security Forum (ISF)

Steve Durbin is Managing Director of the Information Security Forum (ISF). Formerly at Ernst & Young, Steve has been involved with IPOs, mergers and acquisitions of fast-growth companies across Europe and the USA. Having previously been senior vice president at Gartner, he has advised a number of NASDAQ and NYSE listed global technology companies.

Cybersecurity in an Insecure World

Over the coming years organisations will experience growing disruption as threats from the digital world have an impact on the physical. Invasive technologies will be adopted across both industry and consumer markets, creating an increasingly turbulent and unpredictable security environment. The requirement for a flexible approach to security and increased resilience will be crucial as a hybrid threat environment emerges.

The impact of threats will be felt on an unprecedented scale as aging and neglected infrastructure is attacked and disrupted due to vulnerabilities in the underlying technology. Mismanagement of connected assets will provide attackers with opportunities to exploit organisations.

A recent study from the Economist Intelligence Unit (EIU) found that the speed of technological disruption is making it difficult for regulators to keep pace, and there is a need for more, sensible regulation of technology to safeguard innovation and the benefits of today's connected society.

However, new regulations will not be able to keep up and fully address the new challenges posed by exponentially advancing technology and its impact on society. Despite early attempts to pass meaningful regulation, the IoT will grow beyond the ability of any government to secure it. A lack of international regulations will be a wide cause for concern, with new and conflicting regulations causing strategic headaches for many organisations: laws designed to protect individual privacy will clash with those designed to make data processing more transparent. Identifying who holds accountability and liability for security will become less clear

The arrival of 5G, with significantly faster speeds, increased capacity and lower latency, will change existing operating environments. However, these benefits will come at the expense of an exponential growth of attack surfaces. The 5G-enabled devices and networks that underpin society will be compromised by new and traditional attacks, causing chaos and plunging business into disarray.

Critical national infrastructure (CNI), IoT manufacturers, businesses and citizens will all be heavily or totally depen-

dent on 5G to operate. From nation states aiming to cripple CNI – to hackers spying on private networks – 5G technologies and infrastructure will become a key target.

Highly sophisticated and extended supply chains, including cloud technology, present new risks to corporate data as it is necessarily shared with third party providers. IoT devices are often part of a wider implementation that is key to the overall functionality. Since so much of our critical data is now held in the cloud, this opens an opportunity for cyber criminals and nation states to sabotage the cloud, aiming to disrupt economies and take down critical infrastructure through physical attacks and operating vulnerabilities across the supply chain.

In the face of these mounting global threats, organisations must make methodical and extensive commitments to ensure that practical plans are in place to adapt to major technological changes. Employees at all levels of the organisation will need to be involved, from board members to managers in non-technical roles.

Moving forward, enterprise risk management must be extended to create risk resilience, built on a foundation of preparedness, that evaluates the threat vectors from a position of business acceptability and risk profiling.

Enlightened organisations have now moved to a risk-based approach to managing cyber risk. Why? Essentially because the dangers to an organisation from cyber threats have increased in frequency and severity; more organisations are understanding that cyber is entirely embedded across the business and so a cyber threat is actually a threat to business as opposed to something that can be managed from an IT department. This has resulted in a reality check for many. When digital and physical worlds collide, only organisations that take decisive action will prosper.

Steve Durbin



CONFERENCE MODERATORS:



Oliver Rolofs

Managing Partner connecting trust (Munich)

Oliver Rolofs is Managing Partner of connecting trust, a Munich based communications and strategy consultancy. He looks back on a successful fifteen year's career in politics, business and communications, international conference organization, public affairs and strategy consulting for political decision makers and business leaders. Prior to joining connecting trust he worked as Global Head of Media Relations for the strategy 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. He studied political science, international law and sociology and graduated with a master's degree from the Ludwig Maximilian University of Munich.



Tyson Barker

Deputy Director and Fellow Aspen Institute (Berlin)

Tyson Barker is Deputy Director and Fellow at the Aspen Institute Germany responsible for the Institute's Digital and Transatlantic Program. Barker joined Aspen in February 2017 coming from the Brandenburg Institute for Society and Security (BIGS). Prior to that, he served as Senior Advisor to the Assistant Secretary of State for European and Eurasian Affairs at the US State Department in Washington, D.C. from 2014 to 2015. Prior to joining State, he worked for 6 years at the Bertelsmann Foundation, most recently as the Director for Trans-Atlantic Relations. Barker has a bachelor's degree from Columbia University and a master's degree from the School of Advanced International Studies (SAIS) at Johns Hopkins University.

it-sa 2020
The IT Security Expo and Congress

HOME OF IT SECURITY

SAVE THE DATE

Solutions have a platform: **it-sa 2020**.

Nuremberg, Germany | 6-8 October 2020

it-sa.de **NÜRNBERG MESSE**

OPENING ADDRESS:



His Excellency Margaritis Schinas

Vice-President of the European Commission in Charge of Security Union Europe (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. 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 2014, President Juncker appointed Mr Schinas as the Chief European Commission Spokesperson. Mr Schinas has been working for the European Commission in various senior 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.

KEYNOTE:



His Excellency José Angel Gurría

Secretary-General of the OECD (Paris)

Mr. Angel Gurría has been the Secretary-General of the OECD since 2006. Under his leadership, the Organisation has established itself as a pillar of the global economic governance architecture including its active engagement with the G20, G7, APEC and other international fora. Mr. Gurría has advanced the OECD's impact and relevance in several policy area, focusing on the promotion of better lives through inclusive growth and new approaches to economic challenges. He has also made the OECD more inclusive through new memberships, strengthening the link with key emerging economies and fostering its global outreach. Mr. Gurría came to the OECD following a distinguished career in public service in his native Mexico, including positions as Minister of Foreign Affairs and Minister of Finance and Public Credit in the 1990s.

SIEMENS
Ingenuity for Life

Cybersecurity at Siemens

Protect what you value – with our holistic approach and leading technology expertise.

Find out more: www.siemens.com/cybersecurity

SPEAKERS



Dr Reinhard Ploss

CEO Infineon Technologies (Munich)

Reinhard Ploss is CEO of Infineon Technologies AG, a world leader in semiconductor solutions. Ploss began his career at Infineon in 1986 and has been a member of the Management Board since 2007. In addition to his role with Infineon, Ploss is involved in various functions promoting Germany's technological competitiveness: e.g. as member of the Presidential Board at acatech, the German Academy of Science and Engineering. He also serves as Chairman of the "Working Group Silicon Germany" to ensure Germany's long-term competitiveness with market-leading semiconductors. Actively shaping the digital transformation is important to Ploss. In addition to the economic use of new technologies, his focus is on their benefits for society. Besides other, he is involved in the steering committee of the "Plattform Lernende Systeme", that brings together experts from science, industry and society for fostering Germany's position as an international technology leader and a balanced use of Artificial Intelligence. Ploss studied process engineering at the Technical University of Munich and received his doctorate in 1990.



Kristie Canegallo

Vice President of Trust & Safety Google (Mountain View, CA.)

Kristie Canegallo is Google's Vice President of Trust & Safety, a position she has held since March 2018. In that role, Kristie leads the global team that develops and enforces product policies across Google's portfolio. Trust & Safety works to protect Google's users, prevent abuse across products, and ensure Google is a trusted source of information, content, and interactions.

Prior to joining Google, Kristie served in a range of domestic policy, national security, and management roles in the George W. Bush and Barack Obama Administrations, concluding as Assistant to the President and Deputy Chief of Staff from 2014 through January 2017. As Deputy Chief of Staff, she directed the implementation of the Obama Administration's most complex and consequential policy initiatives. Before that, she worked at the Department of Defense, including in Iraq and Afghanistan. Before joining the U.S. Government, Kristie was an analyst at Goldman Sachs.

Kristie is a member of the J. William Fulbright Foreign Scholarship Board and the board of the United States of Care, a bipartisan health care nonprofit organization. She holds a Master of Arts in Strategic Studies from Johns Hopkins School of Advanced International Studies and a Bachelor of Arts in International Relations from Colgate University.



Kiersten E. Todt

Managing Director Cyber Readiness Institute CRI
(New York City, NY)

Kiersten Todt is Managing Director of the Cyber Readiness Institute, a non-profit that convenes senior leaders of global companies to help small and medium-sized enterprises improve their cybersecurity. She also advises senior executives and Boards on cyber risk management and the role of human behavior in cybersecurity. Ms. Todt is the Scholar at the University of Pittsburgh Institute for Cyber Law, Policy, and Security. She most recently served as the Executive Director of the U.S. Presidential Commission on Enhancing National Cybersecurity and has served in senior positions in the White House and United States Senate, where she drafted components of the legislation to create the U.S. Department of Homeland Security.



Christopher C. Krebs

Director Cybersecurity & Infrastructure Security Agency CISA (Arlington, VA)

Christopher C. Krebs serves as the first director of the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). He previously served as Under Secretary of Homeland Security for the National Protection and Programs Directorate (NPPD), CISA's predecessor organization. He has also served as a senior counselor to the secretary of Homeland Security where he advised department leadership on a range of cybersecurity, critical infrastructure, and national resilience issues. He has been in his current role since June of 2018.

Director Krebs leads CISA's dedicated workforce focused on understanding and managing cyber and physical critical infrastructure risk. CISA serves as the United States' risk advisor, working with partners to defend today and protect tomorrow.

A primary strategy CISA employs to achieve its objectives is strengthening collective defense, which relies on international partners and stakeholders.



Scott Jones

Head-designate Canadian Centre for Cyber Security (Ottawa)

Scott Jones was appointed to the position Head-designate of the Canadian Centre for Cyber Security (Cyber Centre), effective 12 June 2018. The Cyber Centre will be a 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. Scott began his career at CSE in 1999 and has held various positions including Assistant Deputy Minister of IT Security, acting Assistant Deputy Minister of Corporate Services and Chief Financial Officer, Director General of Cyber Defence and a variety of positions of increasing responsibility across CSE, primarily in the Signals Intelligence and IT Security Domains. He previously worked at the Privy Council Office as a National Security Policy Advisor in the Security & Intelligence Secretariat.

Scott holds a Bachelor of Applied Science in Electronic Systems Engineering, a Bachelor of Science in Computer Science, and a Masters of Business Administration.



Patricia Zorko

Deputy National Coordinator for Security and Counterterrorism NCTV and Director of the NCTV's Cyber Security Department (The Hague)

Ms Zorko studied at the Police academy, and began working as an inspector with the Utrecht municipal police in 1986. After 20 years of holding various positions she shifted her focus to the national law enforcement and joined the Dutch Police Services Agency (KLPD), where her duties included cybercrime and digitization.

In 2015 Ms Zorko made the transition to the Ministry of Justice and Security. As Deputy National Coordinator for Security and Counterterrorism, she contributes to both national and international security. Her work as Director of the Cyber Security Department focuses on digital protection. Ms Zorko's decision to vigorously spotlight cyber security has resulted in the Dutch Cyber Security Agenda, to which public and private sector parties are committing themselves to further enhance the Netherlands' approach to cyber security.



Ciaran Martin

CEO National Cyber Security Centre (London)

Ciaran Martin was announced as CEO NCSC on 15 March 2016, having previously held the role of GCHQ's Director General for Cyber Security since February 2014. As CEO NCSC, Ciaran leads the public-facing London centre, the UK's technical authority on cyber security, aiming to make the UK the safest place to live and do business online. Since he joined GCHQ, Ciaran has led the transformation of GCHQ's security mission into an active and supportive role for Government departments and critical national infrastructure and has worked to make GCHQ's technical expertise and advice more widely available. Until April 2016 he was also the GCHQ Board member responsible for GCHQ's strategy for managing information risk and has led on policy and communications for the Department. Prior to his role at GCHQ, Ciaran spent eight years in the Cabinet Office as Constitution Director, Director of Security and Intelligence and Principal Private Secretary to the Cabinet Secretary. Ciaran has also held a variety of policy roles at HM Treasury and spent three years in the National Audit Office. Ciaran graduated from Hertford College, Oxford in 1996 with a first in history.



Michael Punke

Vice President Global Public Policy Amazon Web Services (U.S.A.)

Michael Punke is Vice President for Global Public Policy, Amazon Web Services with more than 25 years of experience in international trade and regulatory issues. Punke served from 2010 to 2017 as Deputy US Trade Representative and US Ambassador to the World Trade Organization (WTO) in Geneva. He was the lead for the negotiations resulting in the 2013 Trade Facilitation Agreement, the first fully multilateral agreement in the WTO's twenty-year history, and the 2015 Information Technology Agreement, the first WTO tariff reduction agreement in seventeen years. Punke served previously in government as Senior Policy Advisor at the Office of the United States Trade Representative (1995-1996); and Director for International Economic Affairs at the White House National Security Council/ National Economic Council (1993-1995). Punke is the author of the novel, *The Revenant*, a #1 New York Times bestseller. Punke received his BA with distinction in International Relations from George Washington University and his JD with Specialization in International Legal Affairs from Cornell Law School.



Seiji Ninomiya

Director-General for Global Cybersecurity Policy, Ministry of Internal Affairs and Communications MIC (Tokyo)

Mr. Seiji Ninomiya joined the Ministry of Internal Affairs and Communications (MIC), Japan in 1988. He has been in charge of ICT policy for about thirty years. He also has working experience as Director in National Institute of Information and Communications (NICT) North-America Center in Washington D.C., and Counsellor in National Strategy Office of Information and Communications Technology, Cabinet Secretariat. After serving as Deputy Director-General for Cybersecurity and Information Technology Management, Minister's Secretariat, MIC, Mr. Ninomiya was appointed as Director-General for Global Cybersecurity Policy in July 2019.



Shinichi Yokohama

Chief Information Security Officer NTT Group (Tokyo)

Shinichi Yokohama is Chief Information Security Officer (CISO) for the entire Nippon Telegraph and Telephone (NTT) Group. He also has been responsible for cybersecurity public advocacy to talk to thought leaders globally. He has given numerous talks at conferences such as the 2017 G7 ICT Industry Ministerial Multi-stakeholder Conference in Torino, Italy, and the 2019 OSCE Asian Conference in Tokyo, Japan. He published a book, "Business Management and Cyber Security" in 2018. Before starting this role in 2014, he led a team for post-acquisition integration of overseas operations at NTT DATA, Tokyo. Prior to joining NTT, he was with McKinsey Japan to lead its Technology Practice to focus on the telecom and high-tech industries for 18 years. He originally served the Japanese Ministry of Economy, Trade and Industry for eight years after obtaining a Bachelor of Engineering degree (nuclear engineering) from the University of Tokyo. He also has a master's degree in Public Policy from the Kennedy School of Harvard.



Dr Despina Spanou

Head of the Cabinet of the Vice-President EU Commission (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. 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, Mrs. Spanou was responsible for the European Union's cybersecurity policy and law, digital privacy, connected cities and mobility, digital health, eGovernment and electronic identification. As Director for Digital Society, Trust and Cybersecurity, she was also responsible for the implementation of the EU legislation on security of network and information systems (NIS Directive) and for the negotiations of the EU Cybersecurity Act. Mrs. Spanou started her career at the European Commission in 2003. She had previously practiced European law with the Brussels branch of a US law firm. Despina Spanou is a member of the Athens Bar Association and holds a Ph.D. in European law from the University of Cambridge.



Arne Schönbohm

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

Arne Schönbohm took up his position as president of the Federal Office for Information Security (BSI) on 18. February 2016. Arne Schönbohm (born 1969 in Hamburg) studied international business administration at the International School of Management in Dortmund, as well as in London and Taipei. Between 1995 and 2008 he held several senior positions within EADS Germany, now Airbus, most recently as Vice President Commercial and Defence Solutions for EADS Secure Networks. From 2008 to 2016 he was Chief Executive Officer of BSS BuCET Shared Services AG (BSS AG), which advises companies and public authorities in the fields of digitalisation, cyber security and data protection. In addition to this activity, Arne Schönbohm served, beginning in August 2012, for more than three years as president of Cyber-Sicherheitsrat Deutschland e.V., a Berlin-based politically neutral association, that has set itself the task of advising companies, public authorities and policymakers on matters of cyber security and strengthening them for the fight against cybercrime. He is also the author of various books, including "Deutschlands Sicherheit – Cybercrime and Cyberwar" (2011).



Josh Cowls

Research Associate in Data Ethics, Alan Turing Institute (Oxford)

Josh Cowls is a doctoral researcher based at the University of Oxford's Internet Institute. Through his research, Josh explores the ethical and political impact of data and AI on society, with specific interests in AI ethics, the use of AI for social good, social media as a public sphere, and the use of algorithms to deal with online hate speech. As a Research Associate with the Alan Turing Institute's public policy programme, Josh works on translating insights from academia into effective policy frameworks for the ethical use of data science and AI by governments. Josh holds graduate degrees from the University of Oxford and MIT, and has published research in journals including *Minds & Machines*, *Policy and Internet*, and the *Harvard Data Science Review*.



Juhan Lepassaar

Executive Director of the EU Agency for Cybersecurity ENISA (Crete)

Mr Juhan Lepassaar took up his functions as the Executive Director of ENISA on 16 October 2019. He has more than 15 years of experience in working with and within the European Union. Prior to joining ENISA, he worked for six years in the European Commission, including as Head of Cabinet of Vice-President Andrus Ansip responsible for the Digital Single Market. In this capacity, he also led and coordinated the preparations and negotiations of the Cybersecurity Act. Mr Lepassaar started his career in the EU affairs with the Estonian Government Office, leading for five years the national EU coordination system as the Director for EU affairs and EU adviser of the Prime Minister.



Markus Braendle

Head of Airbus CyberSecurity (Munich)

Markus Braendle was appointed Head of Airbus CyberSecurity in July 2017. With over 850 cyber security specialists in Europe Airbus CyberSecurity supports its Government, Defence and Critical Industry customers in their digital journey by providing cyber security services with a focus on "Protect, Detect and Respond". Prior to this position, Markus was Head of Cyber Security within ABB Group where he built a corporate wide cyber security program and was globally responsible for all aspects of cyber security for the ABB Group. Responsibilities included developing and leading a cross-divisional and cross-functional effort to ensure that ABB products and systems fully support customers' cyber security requirements. Since 2013 Markus is also part of the GICSP (Global Industrial Cyber Security Professional) Executive Steering Committee where he's collaborating with several cyber security organizations and reputable security advisors to enhance industry security competence and workforce development.



Sandra Joyce

SVP Global Intelligence FireEye (U.S.A.)

As SVP, Global Intelligence at FireEye, Sandra Joyce oversees intelligence collection, research, analysis and support services for FireEye cyberthreat intelligence customers and the FireEye security product portfolio. Joyce has held positions in product management, business development and intelligence research over the course of 20 years in both national security and commercial industry. Joyce serves in the US Air Force Reserve and is a Faculty Member at the National Intelligence University. She holds a bachelor's degree in foreign language with four master's degrees in cyber policy, international affairs, science and technology intelligence, and military operational art and science. Joyce speaks English, Spanish, and German and lives in Virginia.



Dr Gregor Peter Schmitz

Editor-in-Chief Augsburg Allgemeine (Augsburg)

Gregor is currently editor-in-chief of Augsburg Allgemeine, with a daily circulation of more than 300.000 one of the largest German dailies. Prior to that, he served as Berlin bureau chief of WirtschaftsWoche, Germany's leading business magazine. Previously, he was Europe correspondent for DER SPIEGEL, Germany's newsmagazine, in Brussels - and from 2007 to 2013 as Washington correspondent for the magazine. Gregor was part of SPIEGEL's WikiLeaks and NSA and was awarded the prestigious Arthur F. Burns and Henri Nannen Prize for his reporting. He is a graduate of Harvard University (MPA) and Cambridge University (MPhil) and holds a law degree from Munich University. He also studied at Sciences-Po Paris and earned a doctorate in political science. In 2018 and 2019, Gregor was recognized as one of the „Journalists of Year“ in Germany.



Prof Alex Stamos

Director Stanford Internet Observatory, Stanford University (U.S.A.)

Alex Stamos is a cybersecurity expert, business leader and entrepreneur working to improve the security and safety of the Internet as the Director of the Stanford Internet Observatory. Stamos is an Adjunct Professor at Stanford's Freeman-Spogli Institute, a lecturer in the Computer Science department, and a visiting scholar at the Hoover Institution. As a Chief Security Officer at Facebook and Yahoo and a co-founder of iSEC Partners, Alex has investigated and responded to some of the most seminal events in the short history of cybersecurity, and has been called the "Forrest Gump of InfoSec" by friends. He is working on election security as a member of the Annan Commission on Elections and Democracy and advising NATO's Cybersecurity Center of Excellence. He has spoken on six continents, testified in Congress, served as an expert witness for the wrongly accused, earned a BSEE from UC Berkeley and holds five patents.



Jeff Moss

Founder of DEF CON and Black Hat Briefings (U.S.A.)

A career spent at the intersection of hacking, professional cybersecurity and Internet governance gives Mr. Moss a unique perspective. He created DEF CON, the world's largest hacking conference and is also the founder of The Black Hat Briefings, a global information security event. Mr. Moss is an angel investor to startups in the security space, serves on the Board of Directors for Compagnie Financière Richemont SA., and was a technical advisor to the TV Series Mr. Robot, and Mr. Moss actively seeks out opportunities to help shape the cybersecurity conversation. He is a member of the US Department of Homeland Security Advisory Council (HSAC) and a commissioner on the Global Council on the Stability of Cyberspace (GCSC). He is a Nonresident Senior Fellow at the Atlantic Council Cyber Statecraft Initiative, and a member of the Council on Foreign Relations. In a prior life Mr. Moss served as the Chief Security Officer and Vice President of ICANN, the Internet Corporation for Assigned Names and Numbers.



Sergej Epp

Chief Security Officer Palo Alto Networks (Munich)

Sergej Epp serves as Chief Security Officer, Central Europe, for Palo Alto Networks. In this role, he develops regional cybersecurity strategy and is overseeing cybersecurity operations and threat intelligence across the region. His functional specialties include cyber defense operations, cyber risk management and transformation management. Prior to joining Palo Alto Networks, he spent over a decade in a variety of cybersecurity and investigation roles at a Fortune 50 financial institution. He also founded and led the first group-wide cyber defense center and established threat intelligence-led capabilities and enterprise-wide programs around Security Awareness, Active Defense and Big Data analytics. Sergej is a passionate advocate for cybersecurity and emerging technologies. He participates regularly as a speaker at conferences, teaches cybersecurity to graduates and is an advisor to multiple start-ups.



Joachim Herrmann

State Minister of the Interior, Government of Bavaria (Munich)

Since October 2007 Joachim Herrmann is the Bavarian State Minister of the Interior. From 1983 to 1991 he was the Vice-Chairman of the youth organisation of the German Christian Democrats (Junge Union Deutschland), and since 1987 their deputy national chairman. From 1990 to 2004 he was a member of Erlangen City Council and Chairman of the CSU (Christian Social Union) group from 1990 to 1997. Since 2001 Joachim Herrmann is the Chairman of the CSU Regional Executive of Middle Franconia and since 2003 member of the CSU Party Executive. Since 1994 Joachim Herrmann is a member of the Bavarian Parliament, elected for the constituency of Erlangen. Since 2008 he is the Second Deputy Prime Minister of Bavaria. Joachim Herrmann is Roman Catholic, married and father of three grown-up children.



Steve Durbin

Managing Director Information Security Forum ISF (London)

Steve Durbin is the Managing Director of the Information Security Forum (ISF). His main areas of focus include strategy, information technology, cyber security and the emerging security threat landscape across both the corporate and personal environments. He is a frequent speaker and commentator on technology and security issues. Formerly at Ernst & Young, Steve has been involved with IPOs, mergers and acquisitions of fast-growth companies across Europe and the USA and has also advised a number of NASDAQ and NYSE listed global technology companies. Steve has served as a Digital 50 advisory committee member in the United States, a body established to improve the talent pool for Fortune 500 boards around cyber security and information governance, and he has been ranked as one of the top 10 individuals shaping the way that organizations and leaders approach information security careers. He has also recently been featured on the top 20 most influential list of leaders whose companies have a vision that shapes the conceptual landscape of their respective industries. Steve is a Chartered Marketer, a Fellow of the Chartered Institute of Marketing and a visiting lecturer at Henley Business School where he speaks on the role of the Board in Cybersecurity.



Tom Koehler

Founder and Managing Partner connecting trust (Munich)

Tom Koehler is founder of connecting trust and a recognized cybersecurity visionary leader, strategist and trusted advisor at board level. He focuses exclusively on cybersecurity and integrated risk management, providing strategy, governance, cyber resilience and M&A advisory to a wide range of clients globally. Tom held a variety of senior executive roles with global advisory and technology leaders. These include: partner at EY European Advisory Center and GSA, CEO and CSO at EADS/Cassidian Cybersecurity, Head of Public Sector at RSA Germany, Director of Infosec Strategy & Communications at Microsoft Germany and Country Manager at VeriSign D-A-CH. Tom Koehler is the Vice Chairman of the Non-Profit-Association Security Network Munich.



Yigal Unna

Director General of Israel National Cyber Directorate INCD (Israel)

Mr. Yigal Unna is the Director General of the Israel National Cyber Directorate (INCD). Mr. Unna previously served as Chief Executive Director of the Directorate's Cyber Technologies Unit in the INCD. Mr. Unna has three decades of experience in the Israeli security apparatus, in Sigint-Cyber positions combining intelligence, R&D and operations together with policy and capacity building. Among others roles, he served as Head of the Sigint-Cyber Division in the Israeli Security Agency ("Shin-Bet") directly under the Director General. Mr. Unna holds an MBA (Tel Aviv University) and a BA in History and Management (Tel Aviv University).



Donald D. Parker

Vice President Product Assurance and Security Intel (Santa Clara, CA.)

Donald D. Parker is a vice president in the Intel Product Assurance and Security group and general manager, Incident Response, at Intel Corporation. He is responsible for coordination and execution of Intel's response to product function and security matters, covering hardware and software products and spanning teams from architecture, design, engineering and communications. In previous roles, Parker led global data center and business client engineering organizations developing and implementing key Intel technologies and products. Earlier in his career he designed and managed portions of many of Intel's flagship microprocessors, including Intel® Pentium® Pro processors. Parker earned a bachelor's degree in computer engineering from the University of Illinois at Urbana-Champaign and holds 16 patents in the field of microprocessor and interconnect design.



Natalia Oropeza

Chief Cybersecurity Officer Siemens (Munich)

As Chief Cybersecurity Officer, Natalia Oropeza is responsible for all global Cybersecurity activities at Siemens. Born and studied in Puebla, Mexico, Natalia has about 30 years of experience in the area of Information Technology with international experiences in Mexico, USA and Germany. She holds several academic qualifications and IT certifications and is a founding member of "Women4Cyber", an initiative of the European Cyber Security Organisation (ECSO). Before she started her engagement at Siemens in 2018, she worked as Chief Information Security Officer and Head of the largest IT Transformation Program at Volkswagen Group.



Axel Deininger

CEO Secunet (Munich)

Axel Deininger has been on the board of secunet AG since January 2018 and took over as chairman on June 1, 2019. He is responsible for the business areas strategy, marketing and international sales. From 2007 to 2017, in addition to the technology office at Giesecke+Devrient Mobile Security, he most recently headed the areas of the telecommunications industry and enterprise security & OEM. Deininger started his career at Bosch Telekom, Siemens AG and Infineon Technologies. Deininger holds a degree in industrial engineering and technology management from the TU Karlsruhe and the TU Lappeenranta, Finland.



Prof Claudia Eckert

Managing Director of Fraunhofer Institute AISEC (Munich)

Claudia Eckert is a full professor at Technical University of Munich where she holds the Chair for IT Security in the Department of Computer Science. She is also founder and director of the Fraunhofer AISEC (Fraunhofer Institute for Applied and Integrated Security). The focus of her research and teaching activities is on the areas of operating systems, middleware, communication networks and information security. As a member of various national and international industrial advisory boards and scientific committees, she advises companies, trade associations and the public authorities in all questions of IT security. In several committees she contributes to the design of the technical and scientific framework conditions in Germany as well as to the design of scientific funding programs on the European scale.



Roland Weigert

Vice Minister, Government of Bavaria (Munich)

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

INSTITUTIONAL PARTNERS:

Global Commission on the Stability of Cyberspace

Launched at the Munich Security Conference in February 2017, the Global Commission on the Stability of Cyberspace is a group of 28 prominent, independent leaders in cyberspace from 16 countries, including former co-Chairs Marina Kaljurand (Estonia), Latha Reddy (India) and Michael Chertoff (USA). It engages the full range of stakeholders to develop proposals for norms and policies that enhance international security and stability, and guide responsible state and non-state behavior in cyberspace. It aims to bring the knowledge, expertise and perspectives of private actors and civil society, including the technical community and academia, into the traditionally state-led dialogue in international peace and security in cyberspace, to reflect the multi-stakeholder reality of this space.



Aspen Institute Germany

The Aspen Institute Germany is an international, independent, and non-profit institution, which is committed to promoting value-based leadership with a strong focus on moral decision-making processes concerning foreign and security policy. The Aspen Institute pays particular attention to forming sustainable networks and on the establishment of an open and critical discourse among executives from Europe, the United States of America, as well as from the Western Balkans. Founded in Berlin in 1974, it is part of the global Aspen network, with partners in the U.S., France, Italy, the Czech Republic, Romania, Spain, Japan, India, Mexico, and the Ukraine. Together, the Institutes are committed to addressing the challenges of the 21st century.



United Europe

United Europe is a non-profit, pro-European association set up in 2013 by prominent European businesspeople, politicians and analysts. It was initiated by Wolfgang Schüssel, former Austrian chancellor, and Jürgen Grossmann, a German entrepreneur, who serves as treasurer. United Europe's goal is a strong and competitive Europe which regards the diversity of its cultures and peoples as a source of strength; to build a Europe that ensures peace, liberty and prosperity for the next generation. We believe in the power of ideas and the value of debate. On this basis, the non-profit association organises CEO roundtables, lectures and Young Professionals Seminars and cooperates with other organisations and institutions.



Deutschland sicher im Netz e.V.

Deutschland sicher im Netz e.V. (DsiN) is a nonprofit alliance of large companies and NGOs, providing comprehensive information, awareness campaigns and educational offers to consumers and businesses on issues of IT security. In June 2007 the Federal Ministry of the Interior became DsiN's patron (dsin.de).



German Mittelstand e.V.

German Mittelstand e.V. is an association and business network promoting the very idea of "German Mittelstand", the backbone of the German economy. It acts as a strong network based on personal relationships offering contacts & know-how as well as support in business matters, inspiring and helping SMEs to move forward, especially by addressing future challenges of concern for medium-sized companies.



The Center Digitisation.Bavaria

The Center Digitisation.Bavaria (ZD.B) is a unique platform for cooperation, research and start-ups. It acts as a driving force for all topics regarding digitisation in cooperation with industry, research institutions, associations and further public activities.

ZD.B is supporting and initialising projects and collaborations between universities, research institutions, established and young businesses, associations, founders, governmental departments and public institutions as well as fostering the public dialogue in the area of digitisation.



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



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:

Marina Kaljurand, Silke Lohmann, Veronika Reichl, Sabine Sasse, Bianca Sum, Christine Link, Jonas Rachals, Marcel Lewicki, Ulrike Woenckhaus, Norbert Heider, Wolfgang Baare-Schmidt, Walter Schlebusch and Kristina Kraus

MCSC

This conference was organised by:



Peter Moehring

General Manager
Security Network Munich
Giesecke+Devrient



Oliver Rolofs

Managing Partner of
connecting trust



Charlott Friederich

Assistant to the General
Manager Security Network
Munich



Fabian Bahr

Head of
Government Relations
Giesecke+Devrient

The Munich Cyber Security Conference provides a forum for top-level industry decision makers to meet and discuss the necessary responses to today's cyber security challenge.

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 seven years ago, the network founded the non-profit association "Sicherheitsnetzwerk München e.V." in January 2019. The new association will 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.

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