Security Network Munich

CONFERENCE REPORT

MCSC MUNICH CYBER SECURITY CONFERENCE 2020

www.it-security-munich.net

SIXTH INTERNATIONAL

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
Giesecke+Devrient Creating Confidence
intel
secunet
sic[!]sec CSIRT & CYBER SECURITY SERVICES
itsa
paloalto NETWORKS
Infineon
Google
SIEMENS Ingenuity for life
CMD CTRL Munich 2020
REPLY SPIKE

Institutional partners:

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE
German Mittelstand
United Europe competitive and diverse
Aspen Institute Germany
DsiN Deutschland sicher im Netz
ZD.B CENTER DIGITISATION. BAVARIA

Media partners:

DW
The Security Times

EXECUTIVE SUMMARY

The world is racing full throttle into a connected reality with new technologies like artificial intelligence; cloud, edge and quantum computing; and 3D printing. At the same time, the rise of the Internet of Things – connected cars, toys, appliances, homes, medical devices and even wearables – is creating new threat vectors that threaten not only data confidentiality, integrity and accessibility, but also physical safety. 2020 will accelerate a central paradox of cybersecurity: even as technology becomes more sophisticated and deeply integrated into every aspect of daily life, the vectors of cyber vulnerability are getting higher and growing.

Against this background, the 6th annual Munich Cyber Security Conference brought together numerous expert speakers and over 200 high level guests from Europe, North America and Asia at the Bayerischer Hof to discuss tomorrow's cybersecurity challenges. Three overarching themes emerged from these discussions:

Trust remains the connective issue that holds the digital world together. Effective cyber security requires "all-of-society" approaches based on trust and social cohesion. Building that trust requires evolving definitions of what constitutes critical infrastructure. Already the EU, the US, Japan and other democracies are redefining voting systems and the 5G Internet backbone as critical infrastructure. The COVID-19 crisis has drawn into high relief the security importance of medical supply chains, equipment and hospital infrastructure. It also requires movement to risk-based approaches that emphasis deterrence, protection, and resilience from cyber attacks.

Our threat communication must evolve to meet the moment: Society must move from a "need to know" to a "need to share" imperative. This means created denser information sharing communities– from ISACs and ISAOs to new models of confidential social media platforms like those pioneered in Israel, specifically for CISOs to share threats. Hubs like ENISA are bulking up their work to create greater information sharing as well.

Even in the age of digital sovereignty, cyber cooperation must increase across borders and across sectors: Digital sovereignty is becoming an important policy objective in Europe and globally. But this relates to management and control of digital devices. It is not digital autarky. Quite the opposite, mastering cooperation across borders, sectors and device generations will be key to assuring cybersecurity. Incentives must be developed to encourage private sector actors like IoT manufacturers and supply chain vendors to work together to establish and adopt cyber norms and cooperate with others like governments. Regulation will often be too slow to keep pace with technological development. This is why cybersecurity by design is aided by constant cooperation.

Ultimately, cyber security is a question of vigilance. The threats in the digital world – like technology, itself – are not static. Nor are they hemmed in by borders as the 2017 WannaCry attack demonstrated. The urgency to address cybersecurity has never been greater. It is time for a shift to occur from awareness to action.

WELCOME REMARKS

On February 13, 2020, the sixth annual Munich Cyber Security Conference brought together a diverse group of 250 high-ranking representatives from academia, politics, the security sector and industry. Entitled „Fail safe – Act brave: Building a Secure and Resilient Digital Society," this year's conference addressed three principle cyber security themes: digital sovereignty, critical infrastructure protection, and challenges in providing a safe and secure IoT environment in a world with increasingly hyperconnected systems.

In his welcome remarks, **Ralf Wintergest**, Chairman of the Security Network Munich, highlighted the growing influence of digital connectivity on our physical world. Over the next decade, 5G will transform the very nature of the Internet. Policy-making needs to keep pace and demonstrate sophistication and confidence to address challenges while maintaining trust.

This report was produced by Security Network Munich in cooperation with Aspen Institute Germany.
All rights reserved by Security Network Munich.

AUTHORS

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.

Tobias Jerzewski
Program Officer, Aspen Institute Germany

Tobias Jerzewski is a Program Officer at the Aspen Institute Germany's Digital Program. He has been with Aspen Germany for more than three years working on tech policy, AI and cyber related issues and also contributing to Aspen's Transatlantic and Leadership Programs. He studied European Affairs at SciencesPo Paris and the Free University Berlin focusing on Poland's role within the EU, the European neighbourhood policy and Franco-German Relations. He also has a particular passion for Hannah Arendt's work with a special emphasis on her case for Federalism and the challenges of modern democracy.Tobias volunteers as Head of Partnerships & Development with The Policy Corner, a platform who seeks to empower students and young professionals to raise their voices on current policy challenges.

OPENING ADDRESS

Shifting from the "Need to Know" to the "Need to Share" Mindset

Margaritis Schinas
Vice President EU Commission in charge of Security Union, Europe (Brussels)

Technological development is accelerating, outstripping policy-makers at every level. In Europe, fragmentation is a persistent risk to assuring cyber resilience. While the European approach to security remains fragmented, Commission's responsibility is to establish linkages and cooperation between member states, private actors, civil society and academia. There is a growing willingness of state actors around the globe to use cyber tools to achieve geopolitical aims. Shinas called on the European Union to make the most of its legal tools to protect its values calling for a mindset-shift "from a need to know to a need to share" mentality.

Core elements of the new EU Commission's approach will include Network and Information Security directive (NIS) revisions, new approaches to directives governing critical infrastructure, the creation of a Joint Cyber Unit and a new certification network plan developed jointly with the European Union Agency for Cybersecurity (ENISA). On the 5G front, Brussels will continue to play a key role in shaping the technology's development. The EU's toolbox on 'Secure 5G Networks' helps frame potential risks linked to this technology. Shinas also sees Europe in the position to frame the policy development around AI and to contain the negative effects that may arise from its dual-use nature. Additionally, EU member-state cybersecurity agencies have stepped up cooperation in securing the European elections against hybrid threats, disinformation and misinformation campaigns. Shinas pointed out that these would only have a lasting impact if they include investment in growing the tech and cyber workforce. Shinas concluded by saying that, "we need trust to build a true Security Union in Europe: amongst citizens, amongst member states, amongst member states and Brussels, industry, civil society and policy making."

IMPULSE SPEECH

Google Shifts to Protect Democratic Integrity by Tackling the Grey Zones

Kristie Canegallo
VP of Trust & Safety Google, Mountain View (CA.)

Google is working to support clean, trustworthy spaces online that build trust in elections and markets. Kristie Canegallo shared insights on joint opportunities and challenges on the basis of Google's work on election integrity and consumer trust. Google is intensely fighting the misuse of its platforms in the manipulation of search results, payment fraud, child exploitation and malware. There is a grey zone when thinking about disinformation, hate speech, targeted and hybrid attacks, AI safety that must be delineated in order to provide users with safe products and to retain trust. Google has therefore expanded its investment in election security and integrity for campaigns as well as the transparency for citizens.

KEYNOTE

The OECD working as a way-station for best practice cross-fertilization

José Angel Gurría
Secretary General, OECD (Paris)

The OECD approaches cyber security and digitization through the lens of economic policy and the preservation of democracy. Security incidents like WannaCry have taught us a lot, especially the need to advance and keep pace with the constant changes originating from the digital transformation. Gurría mentioned Artificial Intelligence for which the OECD adopted a range of principles last year addressing security, safety, traceability of outcomes and risk management approaches of AI systems.

The Internet of Things is also creating a new vector of vulnerability, combining connected devices with the potential for physical harm. Together with the massive proliferation of online devices from toys to refrigerators, the market simply does not provide incentives to provide adequate protections. Governments are working with the private sector to develop labels that increase transparency and promote security by differentiating between products. Starting in 2015, the OECD developed a range of international legal instruments on digital security, calling for sustainable and trust-based partnerships among all stakeholders. In order to move from anecdotes to building a strong evidence base, the OECD, like other standard setters, needs more support from businesses and governments to gather data and share information.

IMPULSE SPEECH:

Topographies of Trust in Cyberspace

Reinhard Ploss
CEO Infineon (Munich)

Reinhard Ploss, CEO of Infineon, began by asking how we can reach a level of trust for technology, similar to the one people have in political institutions. Establishing robust trustworthiness in IoT, AI and other areas where complexity is increasing beyond the grasp of most consumers means that companies and governments must create greater topographies of security, identifying areas in need of more rigorous norms and standards and reestablish incentives that prioritize cybersecurity along with swift deployability of new technologies.

FIRST PANEL

Mission Critical: Effectively Protecting Critical Infrastructure

Moderator: **Kiersten E. Todt** (Cyber Readiness Institute CRI)
Chris Krebs, Director Cybersecurity & Infrastructure Security Agency CISA (Arlington, VA)
Scott Jones, Head-designate Canadian Centre for Cyber Security (Ottawa)
Ciaran Martin, CEO National Cyber Security Centre (London)
Sergej Epp, CSO Palo Alto Networks (Munich)
Patricia Zorko, Deputy National Coordinator for Security and Counterterrorism, Ministry of Justice and Security (The Hague)

Government regulations, controls and best practices play a key role in shaping the readiness and resilience of Critical Infrastructure Protection (CIP) in the event of a cyber-attack. Yet, the critical infrastructure of most countries is owned and operated by the private sector. The definition of Critical Infrastructure is also evolving – propelled by interdependencies, the proliferation of IoT, technology, smart homes, cities and grids, connected vehicles and other new forms of wired devices. As such, safety and protection measures are becoming increasingly complex, stimulated by persistent cyber-threats and breaches, new threat vectors and uneven implementation and enforcement.

- **Maintaining dialogue is essential.** As the traditional layers of government work too slowly, public and private actors must work together to achieve the innovation needed in cybersecurity. This concept of "security through collaboration" is applicable both in Europe and North America. As cybersecurity remains a voluntary endeavor, information sharing is crucial. In the private sector, the use of telemetry produces a massive amount of data. From a US perspective, combining these insights with traditional intelligence represents a core challenge and creates a strong case for smart regulation. When regulators transfer expert advice into the economic model, the cybersecurity sector as whole becomes more resilient. When you anticipate a crisis, you need to ensure that the supply chain is kept in the loop. As we share risks globally, we need to see the vital infrastructure protection not only from the national, but also from an international perspective.
- **5G is about risk-management and tradeoffs.** The United Kingdom's (UK) decision to integrate Huawei in its telecommunication network was based on its national context. The threat assessment looks at how much equipment from high-risk vendors can be tolerated within networks. One of the factors the UK looked at is the assumption that Huawei can be subordinated to the will of the Chinese state. In critical functions, high risk vendors are being excluded and it needs at least two to three resilient companies. From a private sector perspective, the Huawei case is about trust and security.
- **Supply chain and technology integration comes with their own risks.** Companies can outsource a service, but cannot outsource risk. Currently, many business processes are being outsourced with no clear understanding of the risk management protocols. In this respect, trust is a weakness. Vulnerabilities are distributed throughout the supply chain. These need to be addressed in a reliable and rational way, for example by fostering effective top-down information transfer. From the US perspective, further efforts have to be made to raise general awareness and to put good practices in place.
- **Definitions of Critical Infrastructure are evolving.** In the EU, a redefinition of CI may transfer to the application of existing laws and regulatory frameworks rather than creating new ones. An important next step will be to implement the new NIS directive and pressing regulators in the different sectors in order to introduce effective standards and norms is an important step to follow. New sectors are constantly under consideration to be reclassified. For instance, election security is now considered a part of CI.






KEYNOTE

Views from Japan

Seiji Ninomiya

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

Ninomiya presented the Japanese vision for cybersecurity, 5G, IoT and the upcoming Olympic games in Tokyo. Regarding the Olympics, the Ministry of Internal Affairs and Communications is carrying out a large-scale security exercise. Long term, 5G and IoT will be enablers for industry 4.0 and the society 4.0. Japan is taking measures against supply chain risks associated with 5G. These include threat analyses by white hat hackers and the use of AI to detect, temper and tackle malicious attacks. In addition, there are tax incentives to support 5G enrollment. According to the cyber observatory at the National Institute of Information and Communications Technology (NICT) based in Tokyo, half of all attacks are on IoT devices. Some of these are due to passwords that can easily be hacked. Japan supports cooperation with Germany and other governments to guarantee IoT safety.

IMPULSE SPEECH:

Topographies of Trust in Cyberspace

Shinichi Yokohama

CISO NTT (Tokyo)

Building awareness for security in the digital space is still a challenge within companies, even in the telecommunication sector. CISOs have to be forward-thinking and have a much longer timeframe for their work with many telco CISOs looking ahead to 6G networks. The importance is to maintain CISO's having an inclusive, bold, and optimistic mindset.

SECOND PANEL

Digital Sovereignty in The Geo-Politics of Cyber Security – A Myth?

Moderator: **Despina Spanou** (European Commission)
Arne Schönbohm, President of the Federal Office for Information Security BSI (Bonn)
Josh Cowls, Research Associate in Data Ethics Alan Turing Institute (Oxford)
Juhan Lepassaar, Executive Director of the EU Agency for Cybersecurity ENISA (Crete)
Markus Brändle, Head of Airbus CyberSecurity (Munich)
Sandra Joyce, SVP Global Intelligence FireEye (U.S.A.)

Cyber-attacks have been on the rise for years due to new threat vectors, a proliferation of connected devices, insufficient cyber security frameworks and the lack of cyber governance. What is behind the concept of digital sovereignty and how is it linked to cyber security? China and Russia have both taken steps to nationalize the internet. This so-called splinternet-scenario is a serious threat. A newer concern is data sovereignty, which will certainly be followed by AI sovereignty, as this technology relies on the data held by different actors. It is no longer about the data that comes in, but increasingly about the data that is going out.

- **Definitions of digital sovereignty are divergent and at times contradictory.** From a German perspective, there is no such thing as digital sovereignty. The global digital environment consists of expertise in different areas that encompass different components. To a certain extent, digital sovereignty comes from testing, auditing, and understanding what is happening in order to make independent decisions. Digital sovereignty can therefore be achieved in areas in which countries like Germany display strengths, but also evidence interdependence. On the European level, sovereignty is a double-edged sword. One the one hand, it limits a country's influence, but on the other, it allows a country to protect its values and independence. Europe's 5G risk management approach could reflect the balance between interdependence and control. The 5G toolbox consists of a risk distribution approach based on joint risk assessments, or "sovereignty through sharing." This keeps the member states from taking divergent approaches.
- **The private sector takes a less theoretical approach to digital sovereignty.** Security companies experience data breaches daily, from state-backed espionage to cybercrime. The best way to tackle the notion of sovereignty is to broaden the definition beyond ownership to requirements around management, storage and accessibility of data and services that is more operational and grounded in outcome control rather that protectionism.
- **Critical Infrastructure Protection policy is just beginning a new approach to risk management.** This comes with challenges, such as finding the right balance between a holistic and nuanced approach to regulation. It is very likely that we will have an expansion of the NIS-directive to other sectors. With regard to the cloud, ENISA is developing a cybersecurity certification scheme for cloud security providers in order to foster market and user trust. In terms of private data, liability questions are addressed by GDPR. However, industrial data does not fall under this regulation and merits another tool to address it. Experiences from the private sector show that certification can lead to a certain level of confidence and trust, but it is important to strike the right balance between national approaches and certification schemes across Europe.
- **Given the fast pace of technological change, there are some who argue about taking a slow approach to policymaking.** On 5G issue, it is neither about a specific technology nor about a specific country but concerns how we manage the risks surrounding our future infrastructure. In a matter of only 10 years, 5G will probably be a technology of the past. There is a role for truly anticipatory research that can give a sense of what is coming. Foresight remains part of the job of sovereign states and it will remain one of the principles behind running our societies.





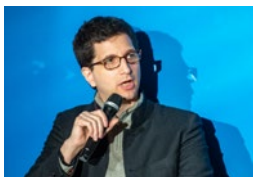


SPOT ON

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.)

2020 is a US presidential election year. Looking back at the 2016 elections, many wonder whether the country has learned from its previous mistakes. This includes general questions about the US election system and disinformation, but also about offensive and defensive hacking capabilities. At the same time, the role and responsibility of platforms like Facebook in the democratic process and regulatory efforts are being discussed, especially in Europe.

- **The US election System is unique in that it is an incredibly decentralized patchwork.** California has strong state legislation compared to several other states – including swing states – that have weak regulatory frameworks. The baseline problem is that every single county must take care of their election security in the cyberspace. It is impossible to guarantee the election safety in all these entities. It is therefore easy to imagine a situation where people doubt the outcome.
- **To successfully counter hackers, it is important to understand their motives.** Many assumed that the 2016 election interference sought to change the outcome, but it could have also just been about casting doubt on the integrity of the process. The slow erosion of confidence in the electoral process is worrisome, regardless of the attacker's aim. Foreign election interference is not always successful. For instance, Chinese interference in the Taiwanese elections ran into the head winds of anti-Chinese public sentiment stoked by the massive protests in Hong Kong. As a result, Chinese disinformation had little effect.
- **In terms of offensive hacking, the US still has the best hackers in the world.** Compared to other countries like China and Russia, which use their hacking power for a broad range of national and economic interests, US hackers are used for narrow military and intelligence purposes. As for defense capabilities, most work in the US is done by companies. China has developed an ecosystem which incentivizes internet companies to fund huge security teams. Some hackers are even treated like celebrities as they win international competitions.
- **On the role of social media platforms, the relationship between the state, the platform and individuals needs to be defined.** What kind of role do democracies want private actors to play the preservation of democratic systems? There is a risk of turning over a considerable amount of our democratic sovereignty to these democratically unaccountable companies if their powers are not defined more concretely. The German NetzDG law effectively privatized powers of the German court system into Facebook, giving a private actor an important amount of state responsibility. Instead of letting the state decide which platform-users to silence, the decision has been outsourced. Regarding election security, private companies cannot replace state regulators and therefore must have specifically defined responsibilities. Europe should also reconsider the balance between anti-competitive behavior and the desire to have highly regulated companies.
- **When it comes to the question of breaking up Facebook, there see two possible tracks.** If the aim is to create a more competitive social media space, there is a good reason to spin off WhatsApp and Instagram. Another approach is to take incremental steps towards regulation around political advertising and introducing tougher liability laws.



GOVERNMENT PERSPECTIVE

Joachim Herrmann

Minister of the Interior, Government of Bavaria (Munich)

Herrmann laid out the agencies and sectoral responsibilities within the Bavarian cybersecurity framework. Core elements of fostering cybersecurity frameworks on a regional, national and international level are a close dialogue and spirit of trust between governments, researchers and the industry. Further measures on a national and European level must be adopted in order to quickly identify attackers and to launch countermeasures.

IMPULSE SPEECH:

Steve Durbin

Managing Director, Information Security Forum ISF (UK)

The increasing number of innovative, tech and data-driven business models could lead to an unnatural societal dependence on technology. The challenge of preserving the data that flows through networks – amplified by the current 5G debate – is not that new. What are possible corporate security implications? As data is widely shared among people, the knowledge of users must be developed. Additionally, data needs to be shared with people who are potential targets. The failure to preserve oversight of the digital ecosystem will prove disastrous.

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)

The number of IoT devices will surpass 25 billion early in this decade. As such, IoT security is a crucial aspect for governments, private actors and consumers. How are governments and the private sector addressing the rising vulnerabilities in this area?

- **Manufacturers still lack incentives to integrate security requirements – even those suggested by regulators – into IoT products.** Code quality remains low. There needs to be more pressure on companies to integrate security by design. Ultimately, it is up to companies to handle their own security problems since they may ultimately be forced to carry the responsibility for their products. This responsibility cannot be passed on to governments and other entities.
- **Businesses implement their own regulations and policies.** But ultimately for supply chain and ecosystem integrity, they must cooperate. Siemens, for instance, has promoted the Charter of Trust with over 16 partners to simplify and accelerate certain mechanisms, including the certification and control of vendors in respective supply chains. Security measures must be implemented now because the fragility in these complex processes and devices places much more at risk than just the vulnerability of the device itself.
- **Regulation of cybersecurity never keeps pace of technological development.** Different approaches should be considered, such as the Japanese or Israel's process-based risk approaches. Additionally, the Israel National Cyber Directorate (INCD) has launched Cybernet, a "Facebook of cybersecurity" which brings together all Israeli CISOs in a confidential social media platform that facilitates real time information sharing.






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

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

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**.

IMPRINT

Publisher:
Security Network Munich

Layout:
Zeilbeck Design Company

© Security Network Munich, 2020
All rights reserved

We look forward to welcoming you to the upcoming

MCSC MUNICH CYBER SECURITY CONFERENCE 2021