Security Network
Munich

CONFERENCE REPORT

MCSC MUNICH CYBER SECURITY CONFERENCE 2022

MCSC MUNICH CYBER SECURITY CONFERENCE 2022
SPRING FORUM
Aspiring to Realizing Cyberspace´s Full Potential –
(Re)Building Trust and Security in a Digital World
Supported by
paloalto
KSG
secunet
infodas
Google
Recorded Future
AIRBUS
MANDIANT
intel
In cooperation with
msc
ISF
ECS
EnSure

www.it-security-munich.net

THIS CONFERENCE WAS ORGANISED BY:

Peter Moehring
Managing Director
Security Network Munich
Giesecke+Devrient

Oliver Rolofs
Co-Founder MCSC

Lorenz Hoeppl
Assistant to the
Managing Director
Security Network Munich

AUTHORS:

Eva Mattes
Aspen Institute Germany

Eva Mattes is Program Officer at the Aspen Institute Germany and part of the Institute's Digital Program. Here, she is responsible for the overall organizational and administrative framework of the program as well as for the design, implementation, and execution of the Institute's high-level events on the most pressing digital topics. Her work primarily focuses on the topics of new technologies, regulation, the digital economy, and digital geopolitics. Prior to joining Aspen, Eva worked at the German Association for Small and Medium-sized Businesses (BVMW) as an expert on digital transformation. Eva holds a Bachelor's degree in Political Science from the University of Heidelberg and a Master's degree in International Relations from the University of Amsterdam.

Stormy-Annika Mildner
Executive Director Aspen Institute Germany

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

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

In Cooperation with:

Bavarian Ministry of Economic Affairs,
Regional Development and Energy

Supported by:

AIRBUS
Giesecke+Devrient Creating Confidence
MYRA Neue digitale Sicherheit
Recorded Future
infodas connect more. be secure.
KSG KREBS STAMOS GROUP
paloalto NETWORKS
secunet
MANDIANT
intel
Google

Institutional partners:

msc Munich Security Conference
CYBER READINESS INSTITUTE
Aspen Institute Germany
invest in bavaria
bitkom
EnSure collaborative
DsiN Deutschland sicher im Netz
Charter of Trust
ISF
ECS EUROPEAN CYBER SECURITY ORGANISATION
UNITED EUROPE competitive and diverse
German Mittelstand
bayern innovativ Innovation leben.
ZD.B CYBER-SECURITY

EXECUTIVE SUMMARY

The cybersecurity threat landscape is changing quickly and dramatically. Studies show that since the outbreak of the COVID-19 pandemic the risk of cyber-attacks has increased worldwide. According to the World Economic Forum and its Global Risk Report 2022 malware and ransomware attacks increased by 358 percent and 435 percent respectively in 2020 (World Economic Forum, 2022). The 2021 mid-year report on cyber-attack trends by the research group of the software company Check Point found that the number of cyber-attacks against organisations globally rose by 29 percent globally in the first half of 2021 (Check Point Research 2021). Measures to contain the COVID-19 pandemic such as isolation, home office, and limited human contact have shifted large parts of human lives and interactions online, boosting connectivity while at the same time creating new vulnerabilities, targets and gateways for cybercriminals.

Moreover, ever-faster digital transformation, including shifting traditional infrastructure to cloud-based solutions, digital connectivity, the Internet of Things, and the increasing use of new technologies such as Artificial Intelligence (AI) make societies more vulnerable to cyber threats. At the same time, cyber-attacks are becoming more sophisticated and complex as well as severe in their impact. This has been especially visible through ransomware attacks, which the Threat Landscape Report of the European Union Agency for Cybersecurity (ENISA) has assessed as the prime threat in 2020-2021. Check Point Research found a 93 percent increase in ransomware attacks in the first two quarters of 2021. Particularly severe attacks, which made headlines around the globe, were the breach of Colonial Pipeline in late April 2021, the attack on JBS Foods, one of the biggest meat processing companies in the world, in May 2021, as well as on Kaseya, which manages IT infrastructure for major companies worldwide, in July 2021. All three attacks had the potential to disrupt key – and critical – areas of the economy on a large scale. According to ENISA, the main cybersecurity threats for the European Union (EU) (April 2020-July 2021) were: Ransomware, cryptojacking, threats against data, malware, disinformation/misinformation, non-malicious threats, threats against availability and integrity, e-mail-related, and supply chain threats.

Cyber security is also more and more becoming a matter of geopolitics and geoeconomics. While the majority of hackers primarily seems to seek money, many of them are state-sponsored actors of authoritarian regimes, trying to undermine and weaken democracies and their societies. In 2021, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) reported ransomware attacks against 14 of the 16 U.S. critical infrastructure sectors. This included the defense industrial base, emergency services, food and agriculture, government facilities, and information technology sectors. Cyber-attacks are also increasingly utilized in warfare, as in the Russian aggression against Ukrainian territorial sovereignty. While Russian troops assembled along the Ukrainian border, a suspected Russian cyber-attack took down more than a dozen Ukrainian government websites in January 2022.

For those affected, cyber-attacks are costly. According to the WEF's Global Cybersecurity Outlook 2022 report, the cost of cyber-attacks amounted to an estimated 3.6 million dollars per incident. In addition, the IBM Cost of a Data Breach Report states that companies needed 287 days on average to identify and respond to a cyberattack. Cybersecurity Ventures estimated in 2020 that cybercrime costs would grow by 15 percent per year over the next five years, reaching 10.5 trillion U.S. dollars annually by 2025 (2015: 3 trillion U.S. dollars).

Cyber threats severely impact all parts of society – citizens, businesses, civil society organizations, and governments. Governments around the world are therefore working on strategies to increase cyber security. For the EU this involves: enhancing cyber resilience, fighting cybercrime, boosting cyber diplomacy, reinforcing cyber defense, boosting research and innovation, and protecting critical infrastructure. Despite these efforts, severe deficits remain regarding skills, equipment, funding, legislation, and cooperation both within countries and across borders. And while large corporations are well-aware of the risks and are preparing accordingly, small and medium sized companies (SMEs) are still struggling – some with a lack of awareness, others with a lack of instruments and funding.

As cyber threats do not know national borders, cyber security has also become an important issue for international cooperation, being prominently included in the work programs of the G7 and the G20. But a lot remains to be done; and mistrust often seems to be a handicap for deeper cooperation.

Against this background, the 8th annual Munich Cybersecurity Conference titled "Drifting Clouds – Leadership Perspectives on Addressing Evolving Cyberthreats" brought together more than 20 high-level speakers and several hundred selected guests from Europe, North America, Africa, and Asia to discuss leadership perspectives on today's cybersecurity landscape and tomorrow's challenges. Due to the ongoing COVID-19 pandemic, the conference was organized in a hybrid setting. High-ranking representatives from academia, politics, the security sector, industry, and think-tanks discussed current cyber threats, IT security in supply chains, and future cybersecurity challenges.

The conference convened February 17, 2022, thus shortly before the Russian invasion of Ukraine. The following summary must therefore be placed in this context, acknowledging that much has changed since then regarding the severeness and magnitude of cyber risks, attacks, and warfare.

Five key findings emerged from the conference.

KEY FINDINGS

› Cybersecurity is Increasingly Becoming an Issue of Geopolitical Importance

While cybersecurity is still often regarded as a mostly technical issue, the changing nature of cyber threats, the growing number of attacks and their increasing severity show that it is anything but. Rather, it has spilled over to the geopolitical realm. State-backed hackers have attacked critical infrastructure, disrupted democratic systems with disinformation campaigns, held information hostage, and stolen personal data, proprietary information, and state secrets. As the world seems to be more and more divided into two blocks – democracies on one side and autocracies on the other – and as geopolitical tensions are growing rapidly, cyberspace is becoming the new battleground for states. Not only governments but also businesses need to be worried about this trend as trade secrets and intellectual property can also be the target of state sponsored cyber-attacks.

At the same time, cyber-attacks play an increasing role in warfare. According to the Cyber Operations Tracker of the Council on Foreign Relations, 34 countries are suspected of sponsoring cyber operations since 2005 (2005-2020), with the large majority originating in China, Russia, Iran, and North Korea (77 percent of all suspected operations). The think-tank recorded 76 operations in 2019, most of them acts of espionage. Apart from espionage, other forms of cyber warfare include sabotage, denial-of-service (DoS) attacks, propaganda attacks, and economic disruptions. Access to accurate information, well-functioning institutions and critical infrastructure are pivotal to stable societies and democracies, and more needs to be done to protect them.

› The Increasing Number and Severity of Cyber-Attacks Require Closer International Cooperation

Cyber-attacks do not stop at national borders. Through global supply chains, the impact of an attack on a single company can quickly spread across sectors and countries, while attackers can hide around the globe. To investigate, track and arrest cybercriminals, national institutions need to increase cooperation with their counterparts in other countries, both bilaterally and multilaterally. New and better-functioning channels of communication are needed to exchange data more quickly, to identify points of vulnerability more effectively, and to develop joint action plans. Furthermore, the interface between law enforcement and the private sector has to be strengthened. All in all, the global community needs to intensify its efforts to find value-based answers to the changing threat landscape. As such, mutual trust, shared rules, and perspectives are key for valuable cooperation.

With the transatlantic economy deepening and the exchange of data playing an increasingly important role, strengthening cooperation between the United States and the EU is pivotal. In summer 2021, the transatlantic partners launched the Trade and Technology Council (TTC). Four of its working groups are dedicated to coordinating information and communications technology (ICT) and data governance. In the light of new legislation being discussed on both sides of the Atlantic and the ambition of the EU to strengthen its sovereignty, the EU and the United States need to ensure that cybersecurity standards, reporting requirements, and subsequent cyber threat assessment do not further diverge. A divergence would not only create new barriers to businesses but also create new vulnerabilities.

› Cybersecurity Needs to be Strengthened Across Sectors and along Value Chains

The globalization and digitalization of supply chains have been a growing concern for cybersecurity experts. Thus, an attack on a single supplier can trigger a chain reaction and compromise a network of providers – within and across borders. While large companies usually implement high levels of IT-security, this is often not the case for SMEs within their supply chains. As IT-security can be costly in terms of soft- and hardware as well as workforce, many smaller businesses still lag behind in implementing necessary measures. This provides cybercriminals with easy access points which can also affect larger companies and critical infrastructures. Thus, businesses, business associations, and governments need to strengthen their joint efforts in addressing weak links in cybersecurity and supply chains by raising more awareness and improving cybersecurity capabilities. More and more companies are also implementing zero trust in cyber security. Following the motto "Never trust, always verify", zero trust is a paradigm shift in the security approach: Every single data access is verified – dynamically, risk-based, and context-sensitive. Businesses are also striving for a more holistic approach, breaking down existing IT silos.

A particular focus needs to be placed on open-source software. While open-source software offers great advantages such as interoperability, vulnerabilities in widely used open-source components pose severe risks to supply chains (including excessive access and code vulnerabilities, lack of dedicated support teams, lack of verification). Therefore, public and private actors must take more responsible for moderating the security of open source.

KEY FINDINGS

› Governments and the Private Sector Must Work Together to Enhance Cybersecurity Through Standardization, Certification, and Legislation

Public-private partnership is the key to preventing future attacks. While the private sector has enormous knowledge of its own companies, the government has capabilities in understanding nation-state activity. As governments must quickly bring regulatory frameworks up to date in order to more effectively target cybercriminals and ensure the needed level of IT-security, they should do so by cooperating more closely with the private sector. To guarantee interoperable cybersecurity between businesses and across borders, public and private actors must thrive for global standards and certification procedures.

› Trust, Diversity, and Education are Essentials to Counter Cyber Threats

While cybercriminals have grown in number and sophistication, human error is still one of the prime causes for the success of cyber-attacks. Verizon’s 2021 Data Breach Investigations Report, analyzing 5,258 confirmed data breaches in 88 countries globally, found that 85 percent of data breaches involved a human element. At the same time, many businesses and state agencies still do not train their employees sufficiently to implement the necessary cyber hygiene. Required training is essential and should be implemented for all employees. Additionally, a good work environment with a culture of core values, including trust, inclusion, empowerment, and diversity of thought is key for good cyber hygiene within organizations. But cyber education needs to start earlier on. Digitization and cyber hygiene should be integrated into the curriculum of schools and dual education schemes. Moreover, public and private actors should implement mentoring and youth programs. Governments should foster such projects by providing funding.

WELCOME

Ralf Wintergerst

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

In his welcome remarks, Ralf Wintergest offered three interpretations of the conference's motto "Drifting Cloud". First, as a weather phenomenon and, therefore, as a symbol for collective action needed to counter current and future challenges of climate change. Second, in connection to dark clouds and storms, symbolic for the current political environment, such as the impact of the COVID-19 pandemic or the Russian aggression toward Ukraine and the West. Third, clouds as a symbol for IT, cybersecurity, and cloud infrastructure and in conjunction with their capacities to either exacerbate the problems or contribute to their solution. He underlined that with these pictures in mind, this year's MCSC followed four overarching questions: (1) How governments see cybersecurity and what they want to do about that, (2) how to react to the ever-growing number and severity of cyber-attacks, (3) how to better anticipate attacks in the future, and (4) how to make supply chains more resilient. In light of these questions, the MCSC's mission was to foster cooperation, collaboration, and solution-building, particularly in the field of cybersecurity.

KEYNOTE

Margaritis Schinas
Vice President EU Commission (Brussels)

In his keynote, Margaritis Schinas, Vice-President of the EU Commission, laid out the impact on and the role of the EU in the light of increasing cyber threats. He explained that the EU has witnessed major aggressions against its member states and partner countries. He pointed at Belarus, which had been utilizing refugees and human lives to put pressure on the EU, and at Russia's aggressions toward Ukraine. Both attacked the West and its values, Margaritis Schinas stressed. To achieve their goals, both actors had resorted to disinformation campaigns and cyber-attacks. Neither incident should be considered as isolated event as EU members had been facing constant cyber-attacks on businesses and society for years. Perpetrators were no longer just aiming to exert economic pressure but increasingly targeted critical sectors, infrastructure, and public institutions. Margaritis Schinas concluded that all EU institutions needed to focus more on cybersecurity

"I think a key here is to mobilize the full potential of cybersecurity. We need to put cyber out of its tech silo," he stated. To prepare for a deterrent response to cyber threats, the EU had been focusing on three actions: First, establishing a legal framework that is future-proof and enables member states to defend themselves against cyber-attacks. Second, ensuring clear and robust responses to cyber-attacks. To do so, the EU had been investing in cyber defense centers and establishing a joint cyber unit. Third, the EU needed to ensure that there were enough skilled people to develop the technologies it needs, which was currently not the case. Margaritis Schinas concluded his keynote by stressing that while these three measures were of central importance, a common discourse and joint forces among EU members and partners remained indispensable.

KEYNOTE

Jen Easterly
Director Cybersecurity and Infrastructure Security Agency (CISA), (Washington, D.C.)

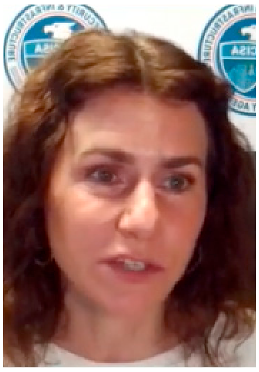
Jen Easterly, Director at CISA, made a point stating that diversity in the workforce fosters a culture of creativity, inclusion, and efficiency, incentivizing employees to thrive. She argued that in the cybersecurity field, culture was the key to success and that this mantra had been standing the test of time throughout her career: Whether as part of the military in Baghdad, where she and others developed a system that helped remove thousands of insurgents from the battlefield, during the time she and her colleagues built the United States Cyber Command, or as director of CISA. Throughout those years, success was not only enabled through operational processes but through the environment that made them possible, Jen Easterly described. Ultimately, cybersecurity was about people, the speaker concluded. An increasingly digitalized world and its connectivity offered tremendous benefits to society, but also created new vulnerabilities. According to the speaker, cybercrimes were becoming more costly and businesses and government both had to invest more to prevent them. At the center of these efforts needed to stand the workforce, Jen Easterly underlined. By stating that "cyber security is not about technology or process or policy, it is about people," she advised creating a good work environment with a culture of core values, including trust, inclusion, and empowerment. This included diversity of thought within organizations, such as allowing employees to work from home or to choose their pronouns. To ward off cyber threats, in the long-run, Jen Easterly emphasized, trust was needed as a foundation to promote and establish good cyber hygiene in organizations.

Mitigating Challenges in An Evolving Cyberthreat Landscape

Moderator: **Kiersten Todt,** Chief of Staff CISA (Washington D.C.)
Lindy Cameron, CEO National Cybersecurity Centre (London)
Arne Schönbohm, President Federal Office for Information Security BSI (Bonn)
Benjamin Ang, Senior Fellow Center of Excellence for National Security (Singapore)
Péter Szász, Deputy Director National Cybersecurity Centre (Budapest)

The global outbreak of the COVID-19 pandemic in 2020 and measures to contain it have been deeply changing everyday lives and the work environment. A growing number of people around the world has been working from home using their private digital infrastructure and, in some cases, even their private devices. This trend has led to growing vulnerability to cyber threats. At the same time, the world is also experiencing an increase in larger-scale ransomware attacks, such as on Colonial Pipeline. Societies and governments around the world are struggling to adapt to these challenges. These developments were put in focus by the first panel of the conference. The speakers also agreed that cyber threats and cybersecurity are increasingly moving into the realm of geopolitics and economics. In this context, the opportunities and threats of the new technology would be discussed on a global stage.

- **According to the speakers, cybersecurity should be viewed as a strategic issue that offered numerous opportunities but also posed considerable risks.** The speakers agreed that the risks needed to be faced heads on by raising awareness, fostering knowledge, and advancing skills for better cyber hygiene. Benjamin Ang warned that if people were not equipped either with adequate technology or with reliant information, it would be difficult for them to protect themselves. Large-scale ransomware attacks were increasing in severity, including targeting healthcare facilities, and posing a direct threat to human lives, the speakers agreed. At the same time, attackers were increasingly operating on a larger scale and around the globe, making it difficult to detect and counter threats on a national level. Therefore, coordination and communication across border were urgently needed, Péter Szász concluded. This was seen as even more important than additional capabilities. The speakers agreed that there was a need to establish shared values and norms that guide cybersecurity approaches.
- **Another point made in the discussion was that governments and the public sector had to cooperate more effectively.** Cyber security was a shared responsibility of governments and the private sector, the speakers agreed. Governments expected companies to know vulnerabilities within their business and along the value chain. The speakers mentioned examples of corresponding governmental regulations including the Saver Space Cyber Plan in Singapore and the IT Security Act 2.0 in Germany. Arne Schönbohm laid out that in Germany, companies had different responsibilities depending on the sector. Companies in critical infrastructure or defense sectors needed to meet high levels of standards, such as mandatory reporting in the event of an attack. Nevertheless, he stressed that “while we as a government have procurement authority, the big changes come from industry,” which is why the right level of information security could only be found through mutual exchange between the public and private sectors.
- **The speakers agreed that cybersecurity was a multidisciplinary topic that needed to be considered in all sectors from the outset.** Cyber hygiene awareness and skills development needed to start much earlier on, being integrated into the curriculum of schools and dual education schemes. The speakers also proposed cross-curricular voluntary youth and mentoring programs. Teachers played a key role, as they often lacked cyber skills, the speakers pointed out. Not only businesses needed to invest in their workforce, but governments also had to offer continuous education and training for its employees. A dedicated budget was needed for this as well as promoting greater diversity within the cyber workforce. Moreover, governments and agencies needed to encourage and promote women to apply for jobs to prevent losing highly qualified employees. This point was underlined by Lindy Cameron, who stressed that the cyber workforce needed to be more diverse in many dimensions to better reflect the society.



SECOND PANEL

Scaling Trust and Cyber Resilience in Supply Chains (of SMEs)

Moderator: Alpha Barry, Founder and CEO of secida (Dortmund)
Axel Deininger, CEO Secunet, Chairman of ECSO (Munich)
George Stathakopoulos, VP of Corporate Information Security, Apple (Cupertino)
Arvid Rosinski, CISO Audi (Ingolstadt)
Phil Venables, CISO and VP, Google Cloud (Mountain View)

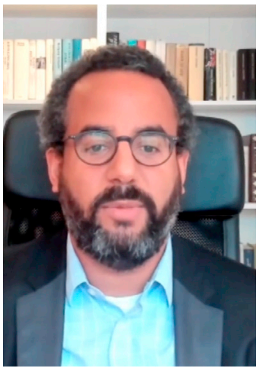
In 2021, more than half a million companies were successfully attacked by cybercriminals globally, Alpha Berry stated, opening the second panel. Even if a company had very high cybersecurity standards, cybercriminals tended to attack a weaker link within the supply chain, which ultimately also breached the company.

› **The speakers agreed that standardization and certification were necessities to create secure supply chains.** Large companies, in particular, relied on countless supply chains that were closely intertwined. As a result, they depended heavily on their business partners and their individual cybersecurity measures. Many of them were in the United States and Asia and had to comply with other rules and standards. For this reason, larger companies often conduct assessments for their suppliers. Moreover, Phil Venables explained, standardization was an important aspect of supply chain security, as it ensured interoperability between companies. He pointed out the SLSA framework, an open standard that organizations could use to assess their supply chains and which Google created based on its internal processes. The other speakers stressed the importance of common standards to create trustworthiness. They agreed that, in general, IT security had to be considered holistically across all areas of a business. Although companies were increasingly aware of this, a lot remained to be done.

› **Open Source had to be secured and maintained as a collective and global effort** – this statement was made by the discussants referring to the Log4g incident, in which a vulnerability was found in a widely used open-source component. Open-source software was of great importance to many companies, but also posed a considerable risk to the security of their software supply chain. Therefore, securing and maintaining open-source software had to be a collective effort, as large parts of the global digital ecosystem were built on the software today. One example was the Open Source Security Foundation, which was founded by a group of companies for the aforementioned purpose.

› **The speakers argued that larger businesses should assist SMEs with their IT security.** Ensuring comprehensive IT-security across businesses required expensive programs that SMEs, in particular, could ill afford. They subsequently reported how their companies helped SME suppliers, who lacked resources and expertise to strengthen their cybersecurity. George Stathakopoulos outlined five principles to get SMEs on the path to improving their security program: (1) training, as basic training is often not available, (2) a general awareness of multi-factor authentication; (3) a robust patching system, (4) enabled logging to know how and if they have been compromised, and (5) incident response, including first steps after an incident occurs.

› **Investment in cyber security should not be seen primarily as a cost factor, but are a cost avoidance factor, since a cyber-attack led to enormous costs for a company per day,** the speakers agreed. Furthermore, companies should not only invest in technology but also in the training of their employees, as they – unknowingly – often open the door to cybercriminals. Arvid Rosinski underlined this by stating: "If you put humans in the center of your strategy, that not only means to invest in technology it means to invest in competencies." As service providers such as cloud providers already often acted as a digital immune system, releasing countless security updates every month, the tools for improved cyber security already existed. For smaller companies, this meant they could defend their security without much effort or cost, the discussant concluded, closing the panel discussion.



Jürgen Stock

Secretary General, Interpol (Lyon)

In his speech, Jürgen Stock laid out, how borderless cybercrime should be fought through global cooperation frameworks. From Interpol's perspective, the past two years had been challenging for law enforcement agencies around the world. The COVID-19 pandemic had greatly changed the operational landscape, especially in the field of cybercrime. Interpol's Cyber Crime 2022 analysis showed that attacks were increasingly tailored and aimed at maximum effect and profit, Jürgen Stock reported. Ransomware was being used against governments and healthcare institutions as a lucrative business model. In summary, the current threat was constant, widespread, pervasive, and borderless. How could law enforcement agencies take them down? How could they help everyone to be better protected? Jürgen Stock outlined the application of a global approach that included three key concepts: Trust, perspective, and shared rules. Regarding trust he explained this meant trust in tools, trust in channels, and trust between partners to have an effective global response to cybercrime.

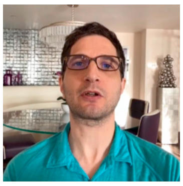
Jürgen Stock stressed that it was crucial to keep in mind that a large part of the world's population did not yet have access to new technologies. This also applied to the respective police and society. In the future, more and more people would use devices that were no longer up to date and created new vulnerabilities. At the same time, he argued, the cyber environment has become increasingly international which required law enforcement to adapt accordingly. "Fundamentally our adversary operates across borders without restrictions. Those tasked with combating the threat, police, governments, and private sector must embrace the same global approach," Jürgen Stock said, summarizing Interpol's vision. Interpol, with its 195 member countries, provided the framework to enforce joint operations. Jürgen Stock explained that the Interpol Cooperation Framework added value to address the threat of cybercrime by securing cooperation channels and networks, providing a central repository for criminal data from all member countries and partners, acting as an interface between law enforcement and the private sector, and enabling more streamlined cooperation between different agencies. Yet, the global lack of a legal framework for cybercrime, particularly joint treaties and cross-border cooperation, remained a key obstacle.

Between a Rock and a Hard Place – Anticipating Future Cybersecurity Challenges

Moderator: **Stormy Mildner,** Executive Director, Aspen Institute Germany (Berlin)
General David H. Petraeus, Partner KKR (New York)
Alex Stamos, Director Stanford Internet Observatory (San Francisco)
Jeff Moss, Founder Black Hat and DEFCON Conference Series (Seattle)

- **The speakers agreed that the frequency and magnitude of cyber-attacks were likely to increase.** Jeff Moss raised the issue of technology in a geopolitical context. Thus, he pointed out that geopolitical tensions and the great power competition between China and the United States increasingly played out in the digital sphere. Cyber space was more and more becoming an arena for influence, competition, hostility and war between nations and other actors. Governments – in particular the Chinese, Russian, and North Korean government – sponsored hackers to steal state secrets, attack critical infrastructure, and disrupt democratic systems. The speakers discussed that operating in cyberspace to target adversaries offered some benefits to these countries in comparison to physical interaction: (1) cyber campaigns, such as misinformation campaigns or Distributed Denial of Service (DDoS) attacks, were comparatively cheap; (2) it was hard to detect operations and attribute these to certain states, thus governments could retain some deniability; (3) such attacks remained under the threshold of armed conflict. While countermeasures were improving, the entire digital ecosystem was getting more complicated, including cloud infrastructure and dual-use components, and new vulnerabilities emerged quickly. That cyber-attacks have become an instrument of modern warfare could be clearly seen in Russia's aggression toward Ukraine, Alex Stamos argued. "One of the big differences between now and previous conflicts is that a huge amount of the command and control that happens with a military like Ukraine's is based upon the civilian network," he explained. He expected Russia to cyber attack critical infrastructure and businesses in Ukraine to weaken the country's resistance but could also affect neighboring countries. He urged policy-makers and businesses in Ukraine and in NATO countries to prepare accordingly. Jeff Moss underlined the special position cyberspace took in modern warfare as the so-called fifth domain, joining land, sea, air, and space. Unlike the other four domains, cyber adapted, and it changed. "Every time we fight in cyberspace or get into a political debate, it will adapt, routs will change, operating systems will be updated," Jeff stressed.
- **General David H. Petraeus further explained that societies had to understand and accept that no single cybersecurity application alone could provide cybersecurity.** He advocated for a comprehensive, integrated, and managed cybersecurity solution based on the principle of zero trust. However, this required an enormous number of applications that had to be integrated as well as constantly updated and monitored. In the future, it would also be essential to share information across borders and between classified sectors at machine speed and based on algorithms to ensure comprehensive responses. Alex Stamos pointed out that the threshold at which an organization was important enough to be attacked was dropping and would continue to do so. Thus, not only large but also small businesses needed to double their efforts to boost cyber security.

The speakers closed the discussion by pointing out that to combat cyber threats in the future, it was critical to share cyber threat data across countries and borders and to strengthen the capabilities of national organizations such as Cybersecurity and Infrastructure Security Agency (CISA) in the United States. In addition, repetitive processes should be increasingly automated to free up capacities and to allow people to focus on higher-value decisions.



KEYNOTE

Moderator: **Gordon Corera,** BBC (London)

Lisa O. Monaco

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

"Cybersecurity is global security," Lisa O. Monaco stressed in her keynote. She advocated that collective cyber defense should focus more on cryptocurrency. According to her, ransomware and digital distortion were only successful if the criminals were paid. Consequently, law enforcement needed to target their sources of income. "We have to bust their business model", Lisa O. Monaco underlined. Many old tools could be used or adapted to conduct cyber investigations. As such, traditional warrants had proven effective in detecting backdoors and disrupting large darknet markets. Lisa O. Monaco reported that following the money was what led to Al Capone in the past and ransomware attackers today. To provide the necessary capabilities, the FBI was currently forming a team specifically dedicated to cryptocurrency. Internationally, the United States and partner countries had launched a virtual currency initiative to share best practices and agree on mutual requirements.

Today's cyber threats required governments and businesses to remain flexible and creative to counter tomorrow's threats. She emphasized that success came from preventing cyber-attacks, not fighting attacks afterward. As the 2016 NotPetya attack demonstrated, cyber-attacks increasingly had global spillover effects that extended beyond the countries they primarily target. To prevent major damage, all organizations should prepare accordingly and strengthen their defenses. Within countries, government agencies also needed the necessary legislative framework to respond to cyber incidents. She further advocated for greater coordination, involving not only national authorities but also international public and private partners. Measures included disruptive capabilities, sanctions, export controls, and early coordination to ensure unity of purpose and response.

TRANSATLANTIC VIEW

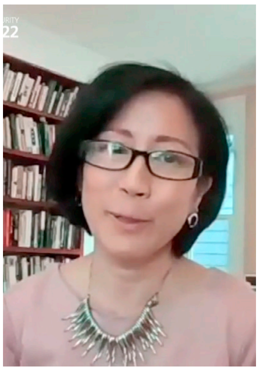
Government Cybersecurity Priorities

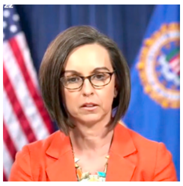
Moderator: **Ellen Nakashima,** National Security Reporter Washington Post (Washington D.C.)
Dmitri Alperovitch, Co-Founder of CrowdStrike & Silverado Policy Accelerator (Washington, D.C.)
Robert Silvers, Under Secretary for Strategy, Policy, and Plans, DHS (Washington, D.C.)
Tonya Ugoretz, DAD Cyber Division, F.B.I. (Washington, D.C.)
Jaak Tarien, Director NATO Cooperative Cyber Defence Centre of Excellence (Tallinn)

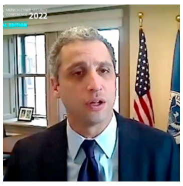
- **The final panel started by addressing Russia's aggressions toward Ukraine.** The speakers agreed that Russia was likely to utilize cyber-attacks targeting Ukraine, NATO, and their allies. From a transatlantic perspective, Russia was expected to try to cut off as many communication links as possible as soon as it launched an attack on the ground. First, to affect the Ukrainian army's command and control structures, and second, to impede communications between Ukrainian governments and their citizens. Cyber-attacks could also be used tactically to cut off communications with the world community and target newspapers or television stations to take them off air or spread fake news, the speakers added.

  Jaak Tarien reported that compared to the situation in 2014, Ukraine was more united and NATO partners stood ready to help the country, which offered a broad array of cooperation options, including training. With regard to possible Russian cyber-attacks on the West, the U.S. Homeland Security Agency was preparing industry and critical infrastructure operators for possible threats, Robert Silvers explained. In terms of international cooperation, partner countries were sharing information, including through NATO, on the latest cyber threats. Dmitri Alperovitch stressed that regarding NATO's defense capabilities, cyber-attacks against member states were included in Article 5, which referred to collective defense. However, this had to be assessed on a case-by-case basis and would largely depend on the attack in question. The experts did not expect Putin to launch a massive attack against the West in cyberspace, but in case he did, NATO was prepared. Concerning disinformation, Robert Silvers explained that this is a common tool Russia used in a conflict. Robert Silvers reported that the current administration enforced an "unprecedented campaign to correct the record and make sure that accurate information is out there to correct the misinformation that Russia spews out."

- **In order to prevent ransomware attacks and money laundering, clear regulation and cooperation were needed across borders, the speakers added.** Looking at the growing threat of ransomware, Tonya Ugoretz explained that the FBI was working with domestic and international partners to take down criminals. As such, the FBI had a close relationship with Europol to identify where the transatlantic partners could conduct joint, coordinated operations. In terms of ransomware attacks, the FBI focused on three central factors: (1) who is behind the attacks, (2) what infrastructure they are using, and (3) where is the money. In terms of preventing money laundering, the United States had trusted partnerships with traditional and virtual financial service providers. At the same time, the speakers highlighted that standards diverged considerably at the international level. To ensure that companies could be compliant with law enforcement agencies, standardization needed to be advanced. To prevent ransomware attacks in the future, governments and their agencies needed to work closely with all entities – both domestically and internationally. This would also require adapting existing frameworks to the digital sphere, the speakers concluded.







Georg Eisenreich

State Minister of Justice, Government of Bavaria (Munich)

Georg Eisenreich closed the MSCS stating that cybersecurity had many dimensions that affect everyone, and that it even had the power to decide over war or peace. Thus, a digital world without borders offered many opportunities, but it also created new dangers. Therefore, cybersecurity was at the top of the agenda for Germany's G7 presidency in 2022, alongside climate change and the COVID-19 pandemic, Georg Eisenreich underlined. Yet, the threat of cyber-attacks was often underestimated by companies, despite the fact that the financial damage from cybercrime was expected to rise to over 10 trillion U.S. dollars by 2025. Companies of all sizes could be attacked, which was why governments and the private sector had to take the necessary precautions. For this reason, Georg Eisenreich added, Bavaria established a central cybercrime unit in 2015, which was responsible for investigating cybercrime throughout Bavaria and also collaborated with other national and international authorities.

Georg Eisenreich concluded by stating that in the light of the growing global cyber threat landscape, this conference had been a central part of a multi-national exchange of views, arguments, and possibilities for cooperation. He thanked all speakers and attendees for an excellent conference and closed the MCSC 2022.

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**.

Security Network
Munich

WRAP UP

Under the title "Aspiring to Realizing Cyberspace´s Full Potential – (Re)Building Trust and Security in a Digital World" the 9th annual Munich Cybersecurity Conference brought together more than 30 high-level speakers and several hundred selected international guests for an in-person event in Munich. In the eye of a changing geopolitical environment, the conference shed light on the possible impact of cyberspace on the security of our countries and essential services. Together with speakers and participants, the conference provided room for constructive and meaningful discussions as well as food for thought for finding answers to pressing cybersecurity issues.

MCSC MUNICH CYBER SECURITY CONFERENCE 2022 SPRING FORUM
Aspiring to Realizing Cyberspace´s Full Potential –
(Re)Building Trust and Security in a Digital World
Supported by
In cooperation with

MAIN TAKEAWAYS

Acknowledging the Mutual Influence of Geopolitics and Cyber

On February 24, 2022, Russia invaded Ukraine, which is considered to be the biggest threat to peace and security in Europe since the end of the Cold War. Experts warn that the return to traditional means and forms of warfare, accompanied by new digital methods of combat, make this conflict particularly dangerous. Cyberspace, thereby, acts as the so-called the fifth dimension of warfare, besides land, sea, air, and space. Unlike the other dimension, cyberspace is not limited by distance and is under constant change. Additionally, the digital sphere enables conflict parties to spread propaganda and disinformation on a large scale through social media platforms.

Considering the enormous possibilities of cyberspace and countless, often Russian led, ransomware attacks such as on Colonial Pipeline in late April 2021, the attack on JBS Foods in May 2021, and on Kaseya in July 2021, many wonder why cyber-attacks have not been playing a large role in Russian warfare. However, what seems like a lack of cyber activity might be just a lack of visible effect. In fact, during the prelude to the Russian invasion, Ukraine faced multiple cyber-attacks on January 14 and February 15, 2022, taking down around 70 government websites, including the Ministry of Foreign Affairs, the Cabinet of Ministers, the Security and Defense Council, and bank services. The lack of severe cyber damage in Ukraine is often attributed to the fact that cyberspace acts as a "Great Equalizer" allowing countries to successfully compete without a large number of conventional weapons.

At the same time, the interpretation of many media outlets declaring Ukraine the winner in the information war against Russia should be treated with caution. This public perception is heavily distorted by filter bubbles and echo chambers. Particularly in many emerging economies and developing nations, disinformation about the war is rampant.

While the importance and impact of cyber warfare in the new conflict environment is still to be determined, digital threats are here to stay and demand an adequate response of democratic and value-based governments, companies, and civil societies across the globe.

MAIN TAKEAWAYS

Building International Cyber Cooperation

Russia’s war in Ukraine marks a return to power politics. The assumption that economic integration and interdependence will eventually prevent conflict and wars, seems to be proven wrong.

As cyber space plays an increasing role in geopolitics and geoeconomics, it is pivotal that governments strengthen their cyber cooperation across borders. While the EU already has a cybersecurity legal framework and sanctions regime in place and is investing in numerous cyber diplomacy enforcement measures, it lacks common cyber defense mehanisms. Current initiatives such as the joint cyber unit proposed by Margrethe Vestager, Executive Vice-President of the European Commission for a Europe fit for the Digital Age, have yet to be implemented. A major hurdle to overcome is the lack of trust between EU member states at the operational level to share cyber expertise when a country is affected by an attack. This problem is fueled by a lack of cyber experts in most countries.

Moreover, some experts argue that alliances such as NATO or the EU have a strategic gap in the cyber domain because most cyber-attacks are considered gray-zone activities and fall below the conventional threshold of an armed attack. As such they would not meet the legal requirements for the institutions’ defense or solidarity clauses. Existing legal frameworks and collaborations need to be reviewed and adapted to the potential impact of the digital sphere. As the cybersphere is not bound by geographic boundaries, cyber cooperation should not be limited to organizations based on geographic proximity. New cooperation formats should be created, base on shared values.

In summary, the changing international security landscape requires adaptation of cooperative networks and regulatory frameworks for cyber resilience.

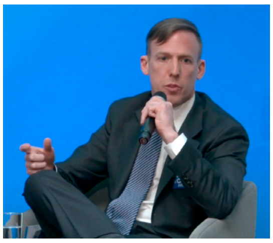
Protecting Digital Infrastructure

The Russian attack on Ukraine has led to a collective awareness of the vulnerability of digital infrastructure. It thereby calls into question the approach of maximal economic benefit, which many countries around the world have followed over the last decade and led to high dependencies on autocratic regimes such as China on many critical resources, hardware, and telecommunications equipment.

To protect digital infrastructure, it is vital that governments, militaries, and businesses recognize their mutual responsibility. However, even if entities can improve their collaboration and develop common standards, norms, and certification processes to enhance the security of systems, cyber-attacks will always remain possible and require an enhanced cyber resilience. Current principles such as security by design and initiatives like the German Cyber Defense Centers are promising steps. Nonetheless, a special focus on cyber-attack responsiveness and more investment is needed. In addition, securing the digital infrastructure requires overcoming the skills gap through collaboration at the public and private level.

New technologies such as blockchain and quantum computing hold both potentials and threats when it comes to protecting critical infrastructure. Ransomware attacks are particularly successful because vulnerabilities are easy to find, cryptocurrencies allow financial transfers outside of law enforcement, and countries like Russia provide criminals with a safe terrain. Timely reporting, an experienced ransomware forensics team, and the immutable nature of the blockchain could help detect and stop ransomware attacks faster.

In conclusion, the vulnerability of digital infrastructure is a long-term problem which is becoming even more complex as innovation is advancing. The only way to cope is by cooperating through nations and sectors and more education and training.



MAIN TAKEAWAYS

Building Trust through Secure International Systems

While the Internet of Things, social media platforms, and greater accessibility to the internet have led to global interconnectedness and greater usability, the system, as a whole, has become more vulnerable to cyber-attacks than ever. A prominent example is the vulnerability linked to the open-source software Log4j. Exposed on December 1, 2021, it has allowed cybercriminals to compromise vulnerable systems with just a single malicious code injection, impacting countless digital products and services globally.

It is vital that government and business entities understand that while they might be competitors, they must engage in a global security community of shared values, in order to counter large-scale cyber-attacks from save harbors. This can be fostered by open source and common standards that allow exchanging best practices and sharing security information.

Moreover, the global community is currently witnessing a severe increase in malware attacks on safety systems and industrial control systems. While it is essential to strengthen defensive capacities, it is also crucial to improve capabilities to react and proactively engage against save heavens. In the Ukraine war, global public-private partnerships of allies have been deployed more successfully than ever. To truly counter cyber-attacks in the long-term stronger international communities based on trust and values must be built up, and cyber resilience must be part of every public or private system.

Securing Systems from the Inside

A poll by the Bitkom e.V. identified that nine out of ten German companies (88 percent) were affected by attacks in 2020 and 2021 (Bitkom Research 2021). Nevertheless, especially in Germany, many companies still lack investment in cyber resilience. As such, the poll also showed that, on average, German companies spend seven percent of their IT resources on IT security, while the association recommends at least 15 percent. While hackers attack from outside, employees often enable them to access a system through malware, lack of cyber hygiene, or security. The human factor thereby connects the cyberspace with the analog world. To prevent cyber-attacks, companies should minimize the human risk of breaches. Digital literacy, in the form of awareness training, testing through fire drills, and education, can function as drivers of trust and must be enforced. It is vital, to create applications and systems that are easy to use, in order to ensure the actual usage.

In addition, the concept of Zero Trust, which follows the principle that no device is inherently trustworthy and must always be verified, has proven to be a game changer. Rather than relying on a firewall, the system requires everyone to identify themselves before access to prevent accidental or intentional attacks. While zero trust may never be fully applicable in practice, the concept should be understood as an overarching principle. As a prominent example, the U.S. government has published a Zero Trust strategy for federal agencies to be implemented by 2024.

Moreover, artificial intelligence (AI) and automation are, to a certain extent, able to replace and support human decision-making and reduce errors within a system. In cyber, AI can be used for processing and analyzing large amounts of data. As such, it is possible to make trust architectures more efficient and less influenced by human error. Nevertheless, its use must always be accompanied by ethical standards, curation, and oversight.

Summing up, fighting external cyber-attacks always requires securing internal systems through minimizing human error, implementing zero trust frameworks, and utilizing innovative technologies.

We look forward to welcoming you to the upcoming

MCSC MUNICH CYBER SECURITY CONFERENCE 2023