Security Network Munich

CONFERENCE REPORT

MCSC MUNICH CYBER SECURITY CONFERENCE 2021

www.it-security-munich.net

Security Network Munich

CONFERENCE REPORT

MCSC MUNICH CYBER SECURITY CONFERENCE 2021

www.it-security-munich.net

7TH INTERNATIONAL

MCSC MUNICH CYBER SECURITY CONFERENCE 2021

Cyber{IN}security – Rethinking Cyber Strategies in Tumultuous Times

Hotel Bayerischer Hof
Munich, April 29-30, 2021

Patronized by:

Bavarian Ministry of Economic Affairs, Regional Development and Energy

Supported by:

paloalto NETWORKS, AIRBUS, Giesecke+Devrient Creating Confidence, secunet, infodas connect more. be secure., ROHDE&SCHWARZ, R&S, itWatch GmbH, Allianz, NOKIA, DRACOON, SIEMENS, deepinstinct, infineon, SentinelOne, ARROW

Institutional partners:

msc Munich Security Conference, Aspen Institute Germany, invest in bavaria, GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE, Charter of Trust, German Mittelstand, EnSure collaborative, United Europe competitive and diverse, CYBER READINESS INSTITUTE, DsiN Deutschland sicher im Netz, DSI DIGITAL SOCIETY INSTITUTE BERLIN, ESMT BERLIN

EXECUTIVE SUMMARY

The Covid-19 pandemic has accelerated digitalization and technology adoption across the globe. At the same time, it has fueled the risk of cyber-attacks and intensified problems posed by new threat vectors, a proliferation of connected devices and insufficient cybersecurity frameworks. It has highlighted the importance of patching in securing tech devices as well as the relevance of secure cyber environments for increasingly international supply chains. The pandemic has turned traditional approaches to cybersecurity upside down and shown that cyber threats are not necessarily novel, but they are becoming more complex and sophisticated.

Against this background, the 7th annual Munich Cyber Security Conference, entitled "Cyber {IN} security – Rethinking Cyber Strategies in Tumultuous Times", brought together over 50 expert speakers and several hundred high level guests from Europe, North America, Africa and Asia in a virtual setting to discuss today's cybersecurity topography as well as tomorrow's challenges. These discussions brought forward three overriding themes:

In the new age of remote working, holistic approaches come to the fore: they constitute the first step towards effective cyber risk management. Such approaches ultimately lead to cyber defense frameworks where cybersecurity and business interests are balanced. Building such frameworks includes a stronger private and public sector cooperation that goes beyond operative threat intelligence and includes insights on tactics and best practices in countermeasures. Controlling the cyber environment is only possible by knowing and measuring the possible risks. Lastly, there is urgency in tackling the skill deficit.

Trust is the gold of the digital age. It constitutes a key factor in breaking down barriers for cooperation between allies. In the context of an increasingly complex cyber threat landscape, establishing sustainable and trusted cyber ecosystems requires more than ever the interplay of diplomatic and technological trustworthiness. Democratic governments with the support of the private sector need to foster multi-level security and cooperation in order to defend cyber systems against malign and disruptive actors to create resilient cybersecurity solutions. Trust and transparency should also guide the EU in its efforts to strive for digital sovereignty, especially towards its friends and partners. Regarding the transatlantic partnership, there is a window of opportunity for stronger EU-U.S. cooperation in the field of cybersecurity as both sides recognize the urgency that emerged from the pandemic.

Ultimately, cybersecurity is a matter of adaptability and identifying trends. The ongoing crisis of disinformation and the hybrid nature of threats is a major challenge for democracy. Within the past decade the distribution of power has undergone significant changes to the disadvantage of democratic allies. In order to defend the societal and technological backbones against nation-state actors like Russia, China, Iran or North-Korea democracies have to catch up with the speed of malign actors. The time has come to join forces and rebuild "trust as the currency of diplomacy".

WELCOME

Ralf Wintergerst

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

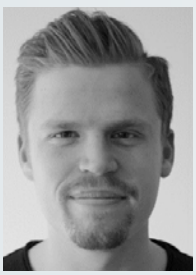
On April 29/30, 2021, the seventh annual Munich Cyber Security Conference (MCSC) took place. Organized in a virtual setting due to the Covid-19 pandemic, the conference entitled "Cyber {IN} security – Rethinking Cyber Strategies in Tumultuous Times" brought together a diverse group of high-ranking representatives from academia, politics, the security sector, and the industry. The conference focused on the increasingly complex cyber threat landscape, fueled by a growing management complexity, a lack of oversight, and resource scarcity. In this sophisticated threat environment, traditional security tactics are failing, existing frameworks need to be reviewed, and new frameworks need to be taken into account.

In his welcome remarks, Ralf Wintergest, Chairman of the Security Network Munich and Group CEO at Giesecke+Devrient, emphasized three particular points that influenced this year's agenda. First, the rise of political tensions, sometimes even among allies. Second, the impact of technologies on our daily lives compared with an unprecedented speed of the global technology race. And third, the Covid-19 pandemic which is far from being over. The MCSC's purpose is to cooperate, to collaborate, and to find common solutions to these challenges particularly in the field of cybersecurity.

AUTHORS

Tyson Barker

Program Assistant, Aspen Institute Germany



Lukas Lorenz has been working at Aspen Germany since April 2019 and is a Project Assistant with the Digital Program since October 2020. Lukas is currently pursuing a master's program in political science at the University of Potsdam. Before joining the Aspen Institute, he completed an internship at the Bildungswerk Berlin of the Heinrich-Böll-Foundation, after which he finished his Bachelor's degree in Political Science and Public Law at the University of Regensburg at the end of 2018. During his bachelor studies he gained international experience in Washington D.C. and Florianopolis in Brazil.

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.

GREETING

The Importance of Trust as "The Currency of Diplomacy"

Wolfgang Ischinger
Ambassador, Chairman Munich Security Conference (Berlin)

The role of digital technology has literally exploded because of the pandemic. After the Covid-19 outbreak at the beginning of 2020, the world is now facing a dramatically changed and new reality. Data is power and will in the future be equal to prosperity. This is a matter for every single person, from citizens to governments and the business community and not just some tech-nerds. Ambassador Ischinger stressed the fact, that Europe needed to become more capable in shaping digital technologies in order to guarantee the security and economic future of its citizens and to promote its own human values. Moreover, the concept of a European (digital) sovereignty will only work with close coordination and cooperation across the Atlantic. Instead of viewing a digitally sovereign Europe as an adversary to the United States, a more capable Europe is to be seen as an asset. Against this background, a common transatlantic digital agenda is in the best interest of both partners. At the core of successful negotiations and a transatlantic digital agenda is the question of how much allies trust each other. Ischinger advocated for more trust between allies as "the currency of diplomacy". The revival of mutual trust must therefore be on top of the agenda on both sides of the Atlantic. Ischinger concluded by raising the question of "How do we promote Europe's digital capabilities while promoting trust across the Atlantic at the same time?" and asked the conference participants to find solutions for this twofold challenge.

OPENING ADDRESS

Strengthening Transatlantic Cooperation through European Sovereignty

Dorothee Bär
Minister of State for Digitalisation (Berlin)

Cyber threats and cyber defense have been of major importance not only since the outbreak of Covid-19. The adaption to current cyber challenges and the adaptation to a new and extremely complex threat landscape is a major challenge for governments. The German state in particular does its best to be prepared for what follows after the current crisis. An important German strategic cybersecurity pillar is the "Cyber Defense Center" – a centralized cooperation, communication and coordination platform for authorities dealing with cybersecurity matters. Another pillar is the "IT-Sicherheitsgesetz 2.0" (IT security act) which passed the German cabinet last year. Because of such initiatives, Minister of State Bär was convinced that Germany is well positioned. But cyber threats and cyber defense forces represent only one corner stone in the vast area of digitization. Another key point is how to meet the challenges of digitization as a whole. The pandemic has bluntly shown Europe's dependencies and weaknesses. The EU must compare itself with the United States and China in order to remain globally competitive in the near future. In many critical areas such as Quantum Computing, AI and new network technologies, Europe has fallen behind other countries. It is time for Europe to strengthen its digital sovereignty together. That means that Europe is aware of their strengths and weaknesses and uses their full potential while minimizing strategic deficits. Instead of protectionism and isolation this approach shows that Europe is part of a globalized world and seeks to strengthen its position on the world stage. Ms. Bär proposed a concrete agenda towards a digitally sovereign Europe consisting of three steps. First, identifying strengths and weaknesses in the digital space with the goal to build up European capacity. Second, the implementation of a specific cybersecurity action plan on a European level. And third, a new way of thinking in business and administration to foster creativity and establish a pioneering spirit.

IMPULSE

Towards a European Cybersecurity Strategy

Cédric Ô
Minister of State for Digital Transition and Electronic Communication (Paris)

Cyber threats are rising. Concerns among democracies about them as well. Cyber-attacks in France have been multiplied by four between 2019 and 2020 and are one of the major challenges for all democracies across the globe. An agenda to tackle those challenges has to contain the following components. First, strengthening the awareness of societies, companies, institutions and governments that everybody is a possible target. Second, investment in technology, start-ups and R&D is key to develop tools that can mitigate the threats. Third, foster cooperation – between the public and private sector as well as on the level of European cooperation. A European strategy for cybersecurity is needed more than ever in order to share knowledge and know-how between states and agencies. The threats and attackers are operating globally and so should democracies to protect a free and open society.

KEYNOTE

Cooperation as Key Element in Fostering Cybersecurity

Her Excellency, Margrethe Vestager
Executive Vice President EU Commission (Brussels)

People, businesses and governments all had to turn digital during the pandemic to pursue their lives and fulfill their duties. Cybersecurity has therefore gained in importance as governments sought to ensure a safe and well functioning online environment. Everyone has a duty in working together: governments have to set the right policy framework; businesses have to make the necessary investments; and citizens have to be aware of what they are dealing with to avoid stepping in the most obvious trap. The European Commission does its best to fulfill its requirements and has adopted a cybersecurity strategy for Europe's digital decade with a number of concrete initiatives in the past year: 1. the network and information system directive; 2. the EU 5-G security toolbox; 3. the European cyber shield. Necessary public and private investments have to be made in order to guarantee the success of those initiatives. Furthermore, a new European cybersecurity competence center and network will be set up in Bucharest which will put together expertise in cybersecurity, research, tech and industrial development to promote the deployment of state-of-the-art cybersecurity solutions. For all of these issues a well-functioning single market for cybersecurity is essential. But making Europe more secure is only one part of the picture in a deeply connected world. For this reason, it is of paramount importance to act as one on the global stage and work closely with likeminded partners. There must be a clear signal to adversaries "if you attack us, you attack all of us and you bear the economic consequences." Herr Excellency Ms. Vestager concluded with a plea that each and every one of us had to be part of the cybersecurity defense, from the individual to the systemic level.

FIRST PANEL

Building Digital Sovereignty in a Multi-Polar World

Moderator: **John Higgins,** President of Chartered Institute of IT, Chair of Global Digital Foundation
Regine Grienberger, Cyber Ambassador Foreign Ministry (Berlin)
Thomas Enders, President German Council on Foreign Relations DGAP (Munich)
Sir Julian King, former EU Commissioner for the Security Union (London)
Hester Somsen, Deputy National Coordinator for Security and Counterterrorism Ministry of Justice (The Hague)

On the European level, a broad debate about digital sovereignty and autonomy has unfolded in the digital and security policy community in recent years. Central to this discussion is, on one hand, the relationship between the EU and the United States, and, on the other side, the competition with China. The latter is of great concern for both the EU and the United States. The Covid-19 crisis has also given additional rise to cyber-attacks and intensified problems posed by new threat vectors, a proliferation of connected devices, insufficient cybersecurity frameworks, and the lack of cyber governance. The panel aimed for two dimensions: first, a broader discussion about digital sovereignty and second, what practical implications this brings about for cybersecurity.

- **The EU needs to balance self-determination and openness.** The EU and its Member States have included the notion "digital sovereignty" in their strategic positioning over the past years. The underlying concept can best be described as follows: The EU needs to build the abilities and capabilities to act on its own if needed but with allies where it can. From a business perspective digital sovereignty can only become a realistic concept if the EU and its Member States start acting in concert. The political approach conceives the term not as a stage to be reached, but a working method to follow. All panelists agreed on the importance of preserving the EU's open character. On the international level, the EU and the United States share the strategic challenge of China. At the same time, it is still difficult to align on many of the common challenges. The EU – U.S. Trade and Technology Council can help synchronize differing approaches on delicate issues. An aspect that clearly provides an opportunity for closer transatlantic cooperation is the cybersecurity challenge.
- **Innovation represents a core driver of technological autonomy,** and the EU has good preconditions. It has to preserve and strengthen its ability to innovate which can only be secured by ensuring that innovated products are being marketed. The private sector calls for a better political assessment of its needs which includes putting less attention on regulative attempts to foster innovation. Investment is crucial when it comes to digital education and skills. Ultimately, the EU must respond to the increasing number of state (sponsored) actors targeting European critical infrastructures, public institutions, companies, and individuals. In this context specific offensive and defensive capabilities – including military ones – need to be developed requiring a more open and effective public-private cooperation.
- **Rule-setting remains one of the EU's main assets.** The concept of digital sovereignty implies the EU's ability to protect its citizens in the digital environment. It touches upon a broad portfolio of realms, such as cybersecurity, IT-security, securing human rights and fundamental freedoms in the digital sphere as well as privacy and data sovereignty. On the international level, Brussels must make sure that EU-rules are being respected. Another strategic asset the EU and its Member States can effectively leverage is the single market: defensively by conditioning access; offensively by setting standards and norms for that market and beyond. The General Data Protection Regulation (GDPR) is a clear example of how the EU can make its own rules respected.

INSIGHT VIEW

Microsoft Pleads for a Better Connected Global Cybersecurity Community

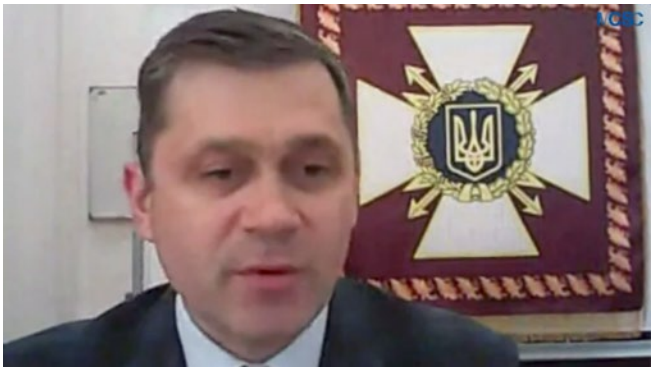
Tom Burt
Corporate VP Customer Security & Trust Microsoft (Redmond, WA)

From the perspective of Microsoft some significant steps had been realized by the global cybersecurity community: First, there is the Paris call for Trust and Security in Cyberspace. Second, a compendium of recommendations on election security. Third, six additional working groups have been established by the French government. Fourth, the Oxford Process and fifth the report of the UN General Assembly to its open-ended working group. On the latter point, Microsoft called for greater emphasis on human rights and a stronger commitment to international humanitarian law. At the same time, it is nevertheless a strong signal that consensus on the international level was possible. Recent cyber-attacks like SolarWinds and Hafnium showed that cooperation between allies is more important than ever. Defense against cyber-attacks of sophisticated criminal groups and state actors gets more and more complicated. Burt concluded by stating that "we need the international community to work together and to impose appropriate sanctions on malign states and actors who violate excepted norms of conducts in cyberspace."

IMPULSE

Building National Cyber Resilience through International Cooperation

Oleksandr Potii
Deputy Chairman of State Service of Special Communication and Information Protection of Ukraine (Kiev)



Cybersecurity is a national and global issue. Cyber-attacks sponsored by states and non-state actors are on the rise. Cyber espionage is an economic and political issue. The number of complex cyber weapons is increasing. At the same time, international humanitarian law is difficult to apply to government action in cyber space. A crucial problem is the attribution of cyber-attacks to specific states. Therefore, more efforts on national and international level are needed. Potii explained that the Ukraine has developed and will implement its cybersecurity strategy 2021-2025 to create the most open, free, stable and secured cyberspace and to promote human rights and freedom as well as to support social, political and economic developments. The goals for the next five years are: 1. Securing the cyberspace to protect its sovereignty. 2. Protection of the rights of freedom and legitimate interest of the Ukrainian citizens in the cyberspace. 3. European and Euro-Atlantic integration in the field of cybersecurity. Building on that, the Ukrainian government has defined three major strategic priorities to guarantee cybersecurity. At first, Kiev seeks to build deterrence potential. Furthermore, cyber resilience for the national security system shall be achieved. Last, the strengthening of cooperation from the national to the international level must be on top of every agenda. Potii concludes with the statement that the "priority of Ukrainian foreign policy is to deepen the European integration process."

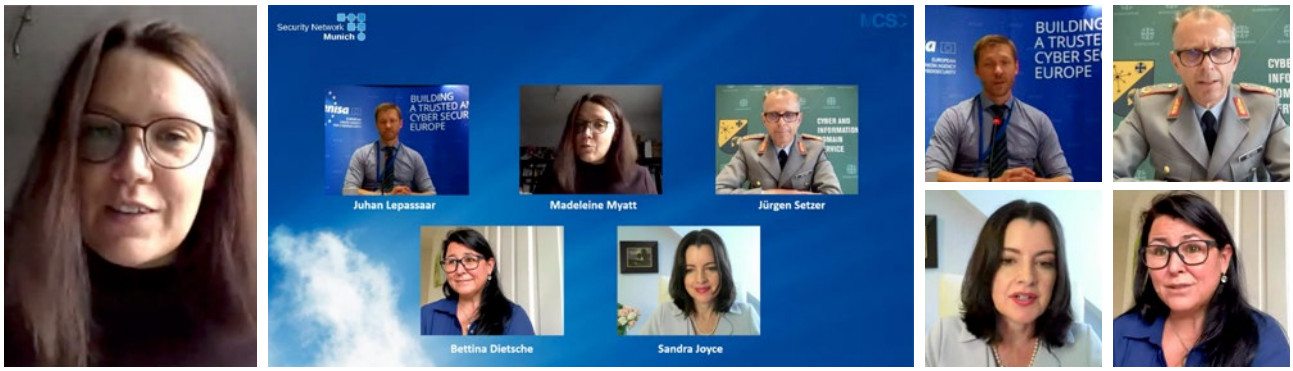
SECOND PANEL

Tumultous Times: Managing Complexity and Gaining Oversight

Moderator: **Madeleine Myatt,** Fellow DGAP
Juhan Lepassaar, Executive Director of the EU Agency for Cybersecurity ENISA (Brussels)
Jürgen Setzer, CISO Bundeswehr (Bonn)
Bettina Dietsche, COO Allianz (Munich)
Sandra Joyce, EVP Global Intelligence FireEye (Milpitas, CA)

The international community is dealing with the constant challenge of an ever-increasing complexity of interconnected information and control systems. Attacks from nation states have been in the public eye. In the current pandemic, strategic attacks on health care facilities are drawing particular attention. Cyber risk management is gaining in importance to cope with this growing opacity and can be discussed from different angles such as system designs and methodology, process-based risk management, legal and standardization frameworks, but also the better understanding of risks and its implications. Are we seeing a new quality of how vulnerabilities are being exploited?

- **Current cyber threats are not novel – but they are becoming more complex and sophisticated.** Experts are identifying three developments. First, attackers are generally looking for increasingly artful ways to distribute their malware, e.g. by inserting it into supply chains. Second, instead of using one attack vector, several attack vectors are being combined to one target. And third, there are spill-over-effects to borders of the cyber realm, e.g. the public revealing of private personal information, known as doxing, is increasingly being utilized. The recurrent question therefore is: have we adjusted our tools and responses accordingly? From the perspective of an insurance company this new kind of sophistication will take root and keep governments, businesses ,and societies occupied even after the pandemic.
- **The problem is not of technological, but of political nature.** Diplomatic relationships have been on an all-time low the last couple of years, to some extent even between allies. Incidents such as the recent Hafnium breach, which are putting thousands of organizations at risk, are calling for stronger cyber diplomacy. These kinds of problems can only be solved on the political level. Within the EU the dimension of collaboration and coordination will be strengthened by the EU Network and Information Security directive (NIS). Ultimately it is about coordinating the Member States' activities and implementing a common methodology. Particularly "normal" organizations with limited capacities can profit from increasing political and cross-border best practice exchange. While we have not seen new tactics, the increased level of audacity and a broader scale in targeting objectives are of new quality. In an ever-uncertain international environment with highly sophisticated attacks from nation states, they need the support of policy makers and the larger international community.
- **Holistic approaches are the first step towards effective cyber risk management.** All panelists agreed on the importance of establishing comprehensive holistic approaches. One of the main challenges remains that basic IT-security knowledge and procedures are lacking in many companies. It is therefore crucial to continue raising awareness of the potential costs that might result from data breaches. Companies need a rigorous end-to-end risk management in place to keep up with the pace of the new technologies. In the EU, the recently adopted European Cybersecurity Competence Network and Centre strengthens the interconnectivity between society and economy in the sector of technology and innovation. The Bundeswehr identifies particular challenges for democratic systems by state actors with hybrid strategies targeting for instance technical networks that can influence public opinions. It is therefore important to look at systems, organizations, and societies to develop holistic approaches across domains.



TRIBUNE

Collective Cybersecurity Mechanisms Instead of National Solo Efforts

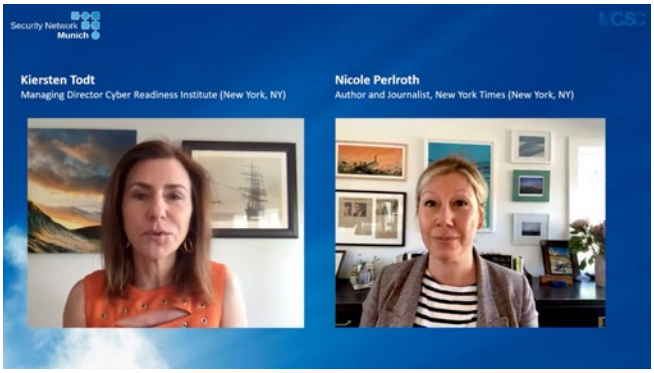
H. E. Prof. Robert Dussey
Minister of Foreign Affairs, Cooperation and African Integration of the Togolese Republic (Lomé)

Emerging technologies redefine boundaries and attributes of power. Therefore, it is essential getting used to uncertainties and try to live with them, in particular because the digital society is a society of hazard and risk and the cyber space a new space of conflict and multiple challenges. Cyber insecurity has not spared Africa, on the contrary, the vulnerability of African companies is increasing. In addition to this, the resilience in several areas is relatively low and the danger immanent. H.E. Dussey was convinced that one of the great challenges in changing Africa lies in the use of digital technologies. These can help improve practices and services to be better protected against cyber-risks and support the knowledge building process on how to find a balance between the use of emerging technologies, protection and regulation. A major problem is that global cyberspace issues are only tackled at national levels. The best way to get ahead of this are more mechanisms for collective cybersecurity and collaboration between parties and security services in Africa as well as cooperation on a global and international level.

SPOT ON

Nicole Perlroth,
Author and Journalist, New York Times (New York City, NY)

Moderator:
Kiersten Todt
Managing Director Cyber Readiness Institute (New York City, NY)



In previous years, governments all over the world have sacrificed cybersecurity in the name of national security and prioritized counter intelligence operations and espionage over international cooperation in the cyber-space. Terms like multi-factor authentication and software updates are still perceived as something rather annoying. Companies do not realize how important it is to develop secure products. This mindset has to change in order to have a chance against the ever-increasing number of cyber threats. Therefore, international cooperation has to be strengthened specifically regarding sanctions for malign state actors. To make this point clear Perlroth presented the following example: "We always ask ourselves 'How will Russia respond to sanctions?' We need to get to a place where we stop worrying about what Putin will think, if we respond to some of these very aggressive cyber-attacks." Serious efforts in hardening defense capabilities – especially when it comes to critical infrastructures – have to be done in the upcoming years. But not only Russian aggression marks a serious problem for democracies. State-financed actors from China, Iran, and North Korea have caught up. The United States is still the world's cyber superpower but at the same time target number one for every malign actor. A readjustment of one's own risk management accompanied with a recalibration of defensive capabilities should be considered as a major issue for the near future. This entails first and foremost the defense of codes that constitute critical infrastructure, because insecure codes are an open door for dangerous cyber-attacks. But instead of penalizing e.g. companies for not being prepared against a number of cyber-risks, governments should provide incentives to accelerate the process of building a more secure cyber space. Perlroth concluded with a call for action: democracies have to be better prepared for the future when it comes to cyber threats. Cybersecurity is much more decisive than the world realizes. Only a combination of strong defense and fearsome offense will lead to a position of strength in an increasingly unstable cyber-security landscape.

CRISIS MANAGEMENT: LESSONS FROM CORONA PANDEMI

Bernardo Mariano

Director Digital Health & Innovation, CIO World Health Organization (Geneva))

The pandemic more than clearly demonstrated that personal and professional cybersecurity is essential for all of us. Cyber attackers work in a very coordinated way and collaborate with each other. It is therefore crucial to work together in order to make sure to remain ahead in this cyber war. Mariano outlined four areas where close cooperation is of major importance: 1. governance; 2. prevention; 3. detection; 4. recovery.

He also named some of the lessons learned from this pandemic: 1. partnering (with computer emergency response teams) is key; 2. partnering with the private sector is key; 3. the need to create a detection mechanism with teams that look constantly where possible vulnerabilities of critical infrastructure are; 4. the importance of investment and training in technology tools.

The combination of people, skills, processes and technology allowed the World Health Organization (WHO) to move from a quite low cybersecurity stand to a more acceptable level. Mariano concluded by emphasizing that "we are not where we would like to be yet. That's why we have to take the lessons of today to be better tomorrow."

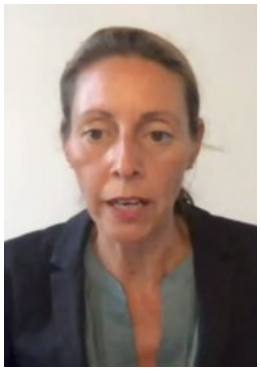
THIRD PANEL

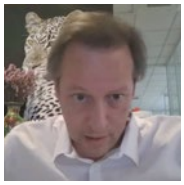
Mitigating Cyber Risks: Engaging Private and Public Agents Successfully

Moderator: **Stormy-Annika Mildner,** Aspen Institute Germany
Edvardas Šileris, Head of the European Cybercrime Centre (The Hague)
Christopher C. Krebs, Founding Partner KS Group (Washington D.C.)
Esti Peshin, General Manager Cyber Division at Israel Aerospace Industries (Tel Aviv)
Jean-Noël de Galzain, President of Hexatrust (Paris)

The Covid-19 pandemic has exacerbated existing cyber-threats and raised new challenges for authorities on the local, national and international level, as well as for industry and civil society. At the same time, the crises can help foster resilience, if public and private actors enhanced their cooperation in order to create synergy effects.

- **The awareness for new cyber threats has not kept pace with the speed of developments.** New technologies represent a threat and an opportunity at the same time. When looking at the current cyber threat landscape one sees no revolution, but evolution. The pandemic has led to an increase in teleworking which exacerbates the existing portfolio of risks, such as the rise of ransomware, business scams, and child sexual exploitation. The modus operandi of governments, enterprises, and even critical infrastructure has changed and involves a stronger cybersecurity dimension. But the necessary level of awareness is missing both in companies and in society as many cybersecurity incidents seem to have no impact on the "real world". We need holistic cyber defense frameworks where cybersecurity and business interests are balanced.
- **Hybrid attacks and the spread of disinformation are the greatest cybersecurity threats democracies are currently facing.** Attacks on and mistrust in democratic institutions are linked to the proliferation of technology throughout the economy in ways our societies do not fully understand. Both the private and public sector are responsible for establishing a transparent and sustainable tech ecosystem that enables people to understand the value brought by these new technologies. Additionally, open discussions about security, safety, sustainability, ecology, and digital protection are needed to foster awareness. All panelists agreed that the internet is fairly regulated which poses a challenge. Finding tangible solutions between public and private sectors is crucial. On the transatlantic level, the Biden administration has started to prioritize cybersecurity issues, namely improving security in the software life cycle and development process. There is clearly a window of opportunity for stronger EU-U.S. cooperation going forward.
- **We need to tackle the skill deficit.** Cybersecurity must be better embedded in the digital ecosystem. In the coming years, a number of new jobs will be created in the field of cybersecurity, i.e. in the context of trusted digital implementations. At the same time the industry will face new regulations asking for stronger protection of personal data and essential systems. In order to keep up with the trusted digital future, public companies and SMEs will therefore have to invest in the creation of new roles. This endeavor should be supported by intensifying collaboration between industry, public organizations, and politics. Cyber resilience is a matter of human resources and of new role models. Leaders need to assume responsibility for cybersecurity – be it on the political level or in the private sector.





DISTINGUISHED GUEST OF HONOR

H.E. Madeleine Albright
Former US Secretary of State

Interviewed by
H.E. Marina Kaljurand
MEP and Former Foreign Minister of Estonia (Tallinn)

Her Excellency Madeleine Albright stressed that the election of Biden as President of the United States is going to have major impacts on the country's role in the future. Biden has a different approach to foreign policy than his predecessor including a broad understanding of its importance. Domestic and foreign policy can only go together, and therefore the transatlantic relationship is essential for "how we work and live together." Regarding cybersecurity it is more than important to define common transatlantic rules and norms to shape cyber systems and technologies such as Artificial Intelligence. In this regard the transatlantic cooperation is essential because digitization and AI affect almost every single area of peoples' daily lives, from the manipulation of elections to the Russian interference in Central and Eastern Europe as well as the behavior of the Chinese regime. Ms. Albright also admitted that the transatlantic partners often disagree on issues like privacy rules and the implementation of data protection. But in the end, they have more in common than any other group of people and therefore have to take a leadership role on this.

Asked about her relevance as female role model, Madeleine Albright stressed the importance of women in the political, business, educational and scientific world. Beyond that, another key issue, especially regarding cybersecurity and new technologies, is the openness of the older generations to learn from the younger ones. She closed with a quote from Robert Frost: "The older I am the younger are my teachers".

OPENING REMARKS

H. E. Ana Brnabic
Prime Minister, Republic of Serbia (Belgrade)

The world around us is becoming faster, more complex and more connected on a daily basis. H.E. Ana Brnabic depicted, that, after entering the office as Prime Minister of the Republic of Serbia, she set clear and ambitious goals to tackle the challenges of a modern world. One of Serbia's top priorities is to guide its economy into a technologically modern and innovation driven future. She emphasized several positive aspects and initiatives aiming at transforming Serbia's education system and public administration. But one must always recognize the vulnerabilities and challenges they certainly implicate. Addressing these is yet another space where governments can play a leadership role.

With all those technological changes, the question of cybersecurity arises and has to be treated with particular emphasis. Serbia takes the protection of its citizens data very seriously. That is why sensitive data has to be stored within the country ensuring the highest safety standards. Government officials are completing cybersecurity training programs to ensure that they develop the skills needed to detect attacks and respond appropriately if needed. H.E. Ana Brnabic concluded by stressing the importance of how crucial international cooperation is when it comes to fighting cybercrime. Enhancing communication among all stakeholders, sharing best practices and participating in the international cybersecurity processes is the only way to ensure safety.

KEYNOTE

Helga Schmid

Secretary General OSCE (Vienna)

Helga Schmidt underscored the role of the current pandemic in forcing the global community to embrace technology and with it its inherent risks at even greater speed. The growing reliance on cyberspace thus raises the likelihood of cyber incidents that may destabilize the already tense relations between states. Regional organizations such as the Organization for Security and Co-operation in Europe (OSCE) are gaining importance in promoting peace and security as well in contributing to cyber stability. This has been underscored earlier this year by the final report of the United Nations open-ended working group on Developments in the Field of Information and Telecommunications in the Context of International Security. One of the OSCE's main objectives is the creation of an atmosphere of trust and confidence by promoting cooperation, reducing misperceptions, and helping prevent escalation that may lead to conflict in the cyberspace. The 57 participating states have adopted sixteen confidence building measures that create and increase transparency, enhance cooperation, and foster greater preparedness by involving many different stakeholders. Instead of drawing conclusions based on incomplete information which could lead to increasing tensions and escalations, the OSCE works towards a framework of rapid information sharing and crisis communication. It includes a network of national points of contact composed of both policy makers and technical experts. Ultimately, it is crucial to extend the dialogue beyond the OSCE framework in order to foster cross-regional approaches. Having adopted their own sets of confidence-building measures, the Organization of American States and the Association of Southeast Asian Nations (ASEAN) together with the OSCE have been encouraged by United Nations to formalize dialogue between regional organizations on these issues in the cyberspace and other fields of action.

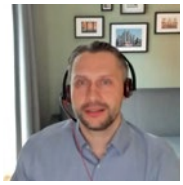
FOURTH PANEL

More Cyber Security through Digital Sovereignty?

Moderator: **Sandro Gaycken,** Director of Digital Society Institute at ESMT
Robert Kośla, Director Dept. Cybersecurity, Chancellery of the Prime Minister (Warsaw)
Werner Strasser, Founder & CEO Fragmentix
Cyril Dujardin, Head of Digital Security, Atos (Paris)
Sergej Epp, Chief Security Officer, Palo Alto Networks (Munich)

Security and sovereignty are having a difficult relationship. On the one side, Europe strives for the best possible and innovative cyber infrastructure. On the other hand, there is a great desire for secure systems without backdoors. Our economies' dependence on China is growing and simultaneously is China's expertise on critical technologies and how to use them against democracies. At the same time, even democratic intelligence alliances such as the five eyes are still in favor of technological backdoors. Against this background, we need to have trusted and trustworthy European sovereign technologies. Additionally, we should aim at a more open and active culture of innovation and better capabilities in critical security functions.

- **Digital sovereignty was described as a controlling influence.** It is always a question of how to influence and shape digital markets such as the European digital single market. More sovereignty implicates more impact and more power to shape the digital sphere in one's own interest. It was also added that it is a question of paradigms. It is important to synchronize the semantic understanding of digital sovereignty. The latter must be thought outside the political sphere to make it possible for the individual, for SMEs, and larger enterprises to have a technology driven chance to achieve and retain digital sovereignty by themselves. From the corporate perspective it was added that customers sometimes have a schizophrenic view regarding digital sovereignty. On the one side, they are asking for sovereignty, i.e. the control of their data, information, and processes. On the other side, they want the optimal protection for their cyber infrastructure. However, it is difficult to offer them both, extensive protection and to be in control without dependency on a third party. By trying to solve this conflict, the panelists agreed on transparency as key factor for sovereignty and security.
- **Combining trustworthy technology, standards, and rules.** Are rules and laws sufficient when it comes to the trustworthiness of technology? From a government perspective it was stated that laws, rules and standards are very important to create trust and set the stage for collaborations between different stakeholders. Declaration of trust without a prove is not valid most of the time. Even though there are specific standards and norms in place there will always be malign actors who do not respect any rules. In order to defend cyber systems against those actors, multi-level security and cooperation between governments and the private sector are sufficient to create resilient cybersecurity solutions.
- **Getting the best out of public private partnerships:** The panelist agreed that the European Union can learn a lot from the United States. The country invested very early in public private partnerships (PPP). Within PPP structures both the private and public sector cooperate and also exchange not only operative threat intelligence but also insights on tactics and best practices in countermeasures. The EU and its Member States have done a very solid first step with initiatives like CSSA and DCSO in Germany or the Cyber Defense Alliance in the United Kingdom. Compared to the United States, the partnership between the public and private sector still remains on a very low level. From the corporate perspective it was added that companies most of the time feel isolated in the EU. A partnership would therefore create much better results because many problems in both the public and private sector are the same. With active dialogue and cooperation those problems and obstacles could be tackled in a more efficient manner.



VANTAGE POINT

Chris C. Demchak

Cyber and Innovation Policy Institute, U.S. Naval War College (Newport, RI)

In the past ten years the distribution of power and influence has undergone significant changes to which the rise in cyber insecurities has made an important contribution. While the physical and digital infrastructure was fairly clear and manageable in 2010, the rise of authoritarian adversaries such as China has changed the situation. Additionally, the growth of cloud computing services largely provided by private firms, added a number of new layers to the existing ecosystem. These developments led to an increasingly complex, less transparent as well as contested global internet. At the same time, democracies do not seem to find appropriate responses to these developments. By creating jurisdictions, they aim at counteracting the decline of westernized influence by making themselves individually defensible against the evolving threat landscape. However, the current approaches are – as Chris C. Demchak noted – not sustainable. Against this background she proposed a different concept with the objective of creating strategic coherence and achieving the scale necessary to resist the Chinese expansion and provide an alternative model. Her concept consists of three operational goals:

- Democracies need to scale up by combining the power of their populations and private sector actors. An integrated whole-of-society defense with allies and their respective information technology (IT) sectors forms democratic IT.
- Democracies need to buy time immediately by starting to collectively defend. Inside this emerging community of like-minded states, the private sector would not have to compete head-to-head with companies such as Huawei as they would not be able to own parts of the stack inside this community.
- Democracies need to start transforming the underlying substrate – the cyberspace we began with – on which all of the Artificial Intelligence and everything else will rest. In order to transform it to what democracies meant it to be, a large research and development effort across universities, governments, and firms is necessary.

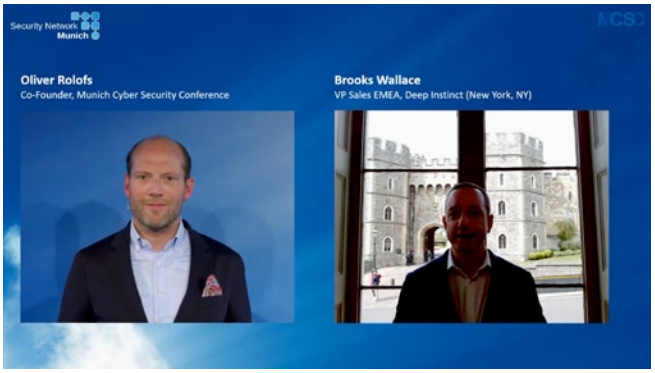
Only then, Demchak pointed out, democracy can be "prosperous, vigorous and united, and provide an alternative counter story to the China model."

IMPULS

Deep Learning – A Game Changer for Cybersecurity?

Brooks Wallace

VP Sales EMEA, Deep Instinct (New York, NY)



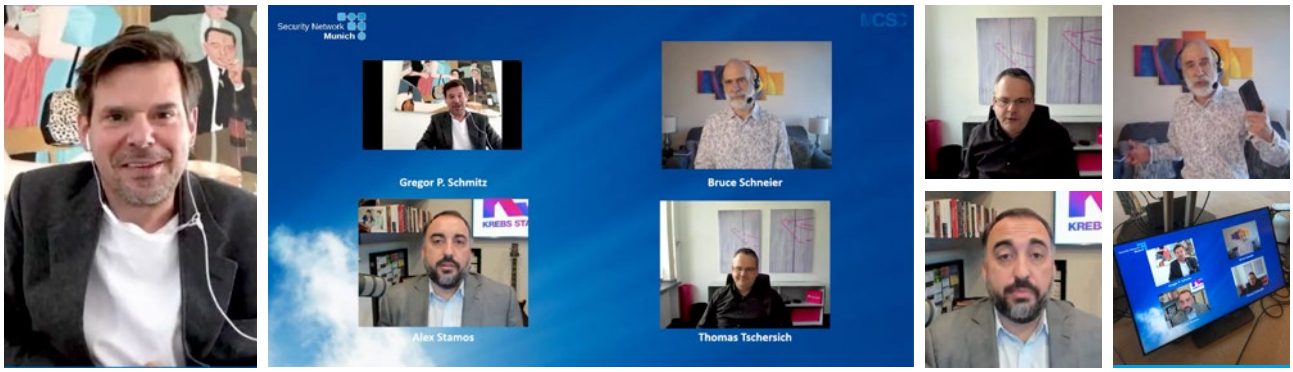
Overnight businesses around the world have changed the way they operate. Suddenly millions of office workers are working remotely, many using their personal smartphones, laptops, and tablets for business. The FBI noticed that cyber-attacks increased by more than 400 percent since the start of the pandemic. According to Brooks Wallace, the cybersecurity measures that are in place until now are antiquated, reactive and have become insufficient. Therefore, the need for disruptive innovation is currently greater than ever before. Security professionals are calling for change, and this is where deep learning comes in. Deep Instinct, in particular, is the first and only deep learning cybersecurity framework that was built for the prevention of cyber-attacks. Deep learning is far more accurate than machine learning. Best of all there is no feature engineering what makes it harder for malware to intrude into the system. Wallace described the race between attackers and defenders as a game of cat and mouse and a war of attrition. Currently, some attackers are ahead of the defenders. Especially nation states have formed small armies under strict discipline to focus on stealing money and government secrets. The only way to outpace the attackers is staying at the edge of innovation, the next wave of cybersecurity, powered by deep learning. He concluded by saying that "if you can't change a game, change the rules and deep learning is allowing us to do just that."

TALKING HEADS

Moderator: **Gregor P. Schmitz,** Editor-in-Chief Augsburger Allgemeine
Bruce Schneier, Fellow and Lecturer Harvard Kennedy School (Cambridge, MA)
Alex Stamos, Director Stanford Internet Observatory, Stanford University (Stanford, CA)
Thomas Tschersich, Chief Security Officer Deutsche Telekom (Bonn)

Cybersecurity is one of the most important issues of our time. Cyber threats and attacks from all sorts of actors have exploded in the past years. Nowadays, everything is digital, and the world is connected through digital technologies. But ensuring the security of digital systems cannot keep up with the fast-paced tech-environment. From a scientific perspective, some key cybersecurity issues are failing, namely the patching of security devices; two-factor authentication; and supply chains with an international industry which is deeply interconnected. One has to trust every aspect of the supply chain but on the other side one cannot trust any of them. Currently there is no optimal solution to any of these security problems.

- **Covid-19 has turned traditional approaches to cybersecurity upside down.** The pandemic has massively accelerated digitalization efforts and was described as the biggest digitization project on the planet. One major impact relates to the flexibility around people's work conditions. The idea of zero trust networks emerged on the agendas of many companies. There was a tendency to build these kinds of corporate networks that would allow employees to work from anywhere while having the same access, telemetry or security benefits as in the office. In reality only a handful of companies implemented such security levels before Covid-19. As a result of the increasing number of employees working from home, immense security gaps opened up especially in cases where people are naively connecting their devices to the internet. Covid-19 demonstrated the loss of control over existing infrastructures and supply chains, which is a serious threat.
- **The fight against cyber threats has to catch up with the speed of malign actors.** Things are getting more complicated, and the risk is increasing. Nation-state actors like Russia, China, Iran, and North-Korea are increasingly aggressive in their cyber-attacks. The panelists agreed that politicians around the world are not aware of the seriousness of these developments and are just running a tech-policy for short-term financial interests. The solutions in tackling these issues differed. From a scientific perspective it was mentioned that there are a lot of technologies but not enough economic incentives for companies to use them. Therefore, more policy to exploit this potential is needed. From a corporate view, it was called for more collaboration among each other to bring together all available knowledge.
- **AI could be a tool to improve future cybersecurity capabilities.** From a scientific perspective this is not a sure thing to say. In the near term, a real benefit is likely because AI can help augment and speed up human response. But in the long term, it is an open question. From the business side, it was added that also attackers will deploy AI technology. Right now, it is an ongoing battle between attackers and defenders. The panelists agreed on the fact that it is a question of overcoming different kind of approaches on the defender's side – irrespective of whether it is about AI, IT-security or IoT security. Today, everything is connected. Especially via internet connections people are milliseconds away from each other, but regulation regimes do not reflect the virtual proximity. This has to be changed in the near future in order to guarantee a sustainable cybersecurity environment.

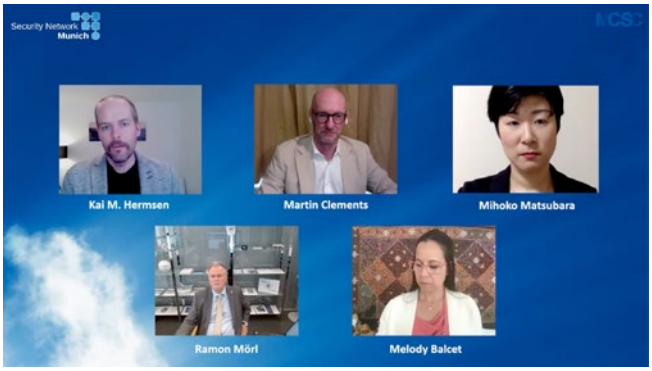


FIFTH PANEL

Moderator: **Kai M. Hermsen,** Director Charter of Trust, Siemens (Munich)
Martin Clements, Security Advisor Credit Suisse (Zurich)
Mihoko Matsubara, Chief Cyber Security Strategist NTT Corp. (Tokyo)
Ramon Mörl, Founder & Chief Executive Officer IT Watch (Munich)
Melody Balcet, Director Operational Risk, Barclays (Washington D.C.)

Data breaches, ransomware attacks, privacy failures, and other cybersecurity risks are part of our everyday life, but companies still seem to struggle with preparing for them. This has a number of reasons: they lack insights on the cyber risks, they might not have the right strategies in place, and they are missing adequate recovery plans. Taking risks in their approaches to risk management is a strategy many organizations seem to have. What are current challenges in corporate cyber risk management and how to cope with them?

- **Cybersecurity risk management is about constantly identifying, prioritizing and measuring the risks.** This entails three basic aspects to follow: do not work in a silo; build up the ability to effectively prioritize; enhance your intelligence capabilities. From the perspective of a Japanese company that acts globally, this goes hand in hand with finding a common global language – for instance the National Institute of Standards and Technology's (NIST) cybersecurity framework – to channel internal cultural differentiations. Another factor not to be underestimated is the role of leadership. Cybersecurity leadership needs to be informed, eager for learning about cutting edge developments and combine the strategic, the operational and the tactical level. Having an additional layer of non-executive oversight of cyber such as dashboards in place is very important.
- **Holistic cybersecurity management incorporates the supply chain and has to be thought globally.** It is a truism that cyber risk management has to be holistic, panelists agreed. Companies need to look at two simple management doctrines: you cannot manage what you cannot measure; and if you would like to measure something you need to know it. In order to reduce possible risks, it is therefore crucial to know what is inside the box. That is why companies should want to understand what hardware and software components are built in their products. There is no added value if the components have any back doors and communicate with actors you do not know. The ambition has to be to get from knowing the supply chain toward building a trust chain. In short, to know exactly what is in the product and how to patch it, is of paramount importance. This task does not get easier in an ever-globalized environment, but has to be challenged.
- **Collaboration is the nuts and bolts of successful cyber risk management.** Breaking down the barriers to collaboration is crucial in budling up trust "as the currency of diplomacy" as Wolfgang Ischinger stated in his opening speech. It includes to establish legal channels that allow you to have conversations with your competitors, to build alliances with your peers, and discuss current challenges as a cybersecurity cohort. There is also a need to rebuild trust in leaders. Top leaders who can persistently combine process technology, behavior, culture, and values can help accelerate collaboration within and beyond the own organization.



SPOT ON

Enforcing Cyber Security – A Legal Perspective

Lisa O. Monaco

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

The number of cyber threats and attacks have exploded over the last couple of years and are therefore on top of Lisa O. Monaco's priority list. Furthermore, they have become more diffuse, more sophisticated and more dangerous than ever before. Regarding cyber threats the United States and other democracies are at a pivotal moment. Malicious actors are exploiting the technology that has been a boon to commerce, free speech, and global communication. By moving all of that from the analog to the digital sphere the security aspect was often neglected. That is one of the reasons why new technologies, innovation and connectivity is being used against free democracies by nation-state adversaries and criminal enterprises. Monaco stated that there is a need to rethink and assess if the most effective strategies are used in the fight against cyber threats. Asked about ransomware Monaco pointed out that last year was of particular severity. There has been a huge financial damage for individuals, small businesses, companies, hospitals, etc. But it is not just about money it is about mayhem, especially when facilities like hospitals or critical infrastructure are under attack. Only with a holistic approach in the fight against those malicious actors it can be guaranteed to be one step ahead of the adversaries. On top of that, working together with partners and the private sector overseas and especially in Europe is key: "We have to get innovative and aggressive, and we have to work collaboratively and cooperatively with our partners and the private sector if we are going to keep pace with what the malicious actors are doing." Especially when it comes to attacks from nation states like China, Russia, Iran and North Korea it is essential to have good partners at your side. Together it is possible to deter, disrupt and sanction malicious acts from nation state actors.

CLOSING REMARKS

Roland Weigert

Vice Minister, Government of Bavaria (Munich)

Digitalization is advancing in giant leaps. The pandemic in particular has accelerated the development of digital solutions. Many people are working from home and are therefore facing the risk of cyber-attacks. To successfully defend against them everyone will need to pull together, and measures need to be rolled out across all levels. The policy of the Bavarian state government's high-tech agenda is to provide targeted support and ensure long-term funding. The security network Munich, launched by the Bavarian Ministry of Economic Affairs was initiated with the intention of providing central support for network initiatives as well as for the users of such technologies. Serving as networking and collaboration hub, the security network Munich enables the active transfer of knowledge between researchers, the private sector and end users. Cooperation on all levels enriches and benefits the work of all people involved in the cybersecurity realm.

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:

Gabi Dreo, Heinz Stiastny, John Mengers, Kai Horten, Falk Herrmann, Tom Koehler, Tobias Jerzewski, Wolfgang Baare-Schmidt, Marcel Lewicki, Silke Lohmann, Robert Naumann, Jacob Freedman, Philippe Delanoue, Ciaran Martin, Steve Durbin, Marina Kaljurand, Thom Langford, Stefan Kägebein, Konstantin Schwalbe, Wolfgang Hackenberg, Andreas Pritchard

This conference was organised by:

Peter Moehring
General Manager
Security Network Munich
Giesecke+Devrient

Oliver Rolofs
Managing Partner of
connecting trust

Fabian Bahr
Head of
Government Relations
Giesecke+Devrient

Kiersten E. Todt
Managing Director Cyber
Readiness Institute

Lorenz Höppl
Assistant to the
General Manager
Security Network Munich

Nina Sandmann
Technical Coordination,
Contagio

Christopher Lass
Web-Design

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 nine 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

We look forward to welcoming you to the upcoming

MCSC MUNICH CYBER SECURITY CONFERENCE 2022