EXECUTIVE SUMMARY

The threat of cyberattacks is greater and more complex than ever. In 2020 and 2021, the COVID-19 pandemic and the associated rapid shift to remote work led to an increase in vulnerabilities as many organizations did not enforce appropriate IT security measures. A survey by bitkom e.V., Germany's digital association, found that 59 percent of the surveyed companies offering the ability for employees to work from home had experienced IT security incidents attributable to remote work since the pandemic began.[1] Since 2021, Russia's war against Ukraine has caused an influx of state-sponsored cyberattacks on Ukraine as well as several other countries. Growing geopolitical tensions, spurred by the systematic competition between China and many industrialized countries, foremost the United States, also increase the risk of cyberattacks. Moreover, new technologies are making cyberspace even more complex, as they offer new opportunities for protection but can also be exploited by cybercriminals.

According to Check Point, the number of global cyberattacks increased by 38 percent in 2022 compared to 2021, reaching an all-time high in the fourth quarter of 2022, with an average of 1,168 attacks weekly per organization.[2] The AI-based cybersecurity company CloudSek found that the number of attacks on the government sector increased by 95 percent globally in the second half of 2022 compared to the same period in 2021.[3] The ENISA Threat Landscape Report assessed that between May 2021 and June 2022 more than ten terabytes of data were stolen by ransomware each month (data reported for the EU, the United Kingdom, and the United States).[4] In a ranking by the World Economic Forum (2023) of the most serious global short- and long-term risks, "widespread cybercrime and cyber insecurity" ranked 8th in both categories.[5]

Cyberattacks are not only increasing in number, scope, and complexity; their cost are also increasing. In 2022, the average cost of a data breach amounted to 4.35 million U.S. dollars, which was a 2.6 percent increase compared to 2021.[6] Further analysis shows that cyber threats are relevant for all sectors. In the EU, the United Kingdom, and the United States nearly 50 percent of incidents in the reporting period of 2021 and 2022 were targeted at public administration and governments (24%), digital service providers (13%), and the general public (12%), while the other half were directed at all other sectors of the economy.[7]

---

[1] Bitkom e.V., German Businesses under Attack: Losses of more than 220 Billion Euros Per Year., 2021, https://www.bitkom.org/EN/List-and-detailpages/Press/German-business-losses-more-than-220-billion-euros-per-year

[2] Check Point Research, Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks, 2023, https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (accessed April 10, 2023).

[3] Hansika Saxena and Aastha Mittal, Unprecedented Increase in Cyberattacks Targeting Government Entities in 2022, in: CloudSek, 2022, p.1, https://cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022 (accessed April 10, 2023).

[4] ENISA, ENISA Threat Landscape 2022, 2022, p. 44, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends (accessed April 10, 2023).

[5] World Economic Forum, The Global Risks Report 2023, 18th Edition, 2023, p. 6, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (accessed April 10, 2023).

[6] Abi Tyas Tunggal, What is the Cost of a Data Breach in 2023?, in: UpGuard, April 6, 2023, https://www.upguard.com/blog/cost-of-data-breach (accessed April 10, 2023);

[7] ENISA, ENISA Threat Landscape 2022, 2022, p. 14, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends (accessed April 10, 2023).

According to CloudSek research, the most targeted countries in 2001 and 2022 were India, the United States, Indonesia, and China, accounting for approximately 40 percent of the total reported incidents in the government sector (followed by Russia, Mexico, Brazil, Saudi Arabia, Columbia, and Ukraine).[8] The origin of cyberattacks is predominantly obscured and untraceable. However, different research shows that Russia and China appear to be a major source of cyberattacks.[9] According to the Cyber Operations Tracker of the Council on Foreign Relations, 34 countries have been 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).

In assessing the current cyber threat landscape, many experts point out the significance of the Russian invasion of Ukraine, which has ushered in a new era of cyberwarfare and hacktivism and led to a significant global increase in cyberattacks in 2022.[10] In its threat report, ENISA connected the Russian war to a significant increase in the activities of partisan hacktivist groups, "cyber actors conducting operations in coordination with kinetic military actions, hacktivist mobilization, cybercrime, and support from nation-state groups".[11] Experts also point out Russia's use of cyber tools to impact military and civilian communications, including blocking public media transmissions and the spread of disinformation. According to data by Google (2023), there was an over 300 percent increase in Russian phishing campaigns directed against users in NATO countries in 2022 (compared to a 2020 baseline).[12] Moreover, the conflict further blurred the lines between cyber actors such as nation-state actors, cyber criminals, and hacktivists, as both sides of the conflict recruited a broad range of cyber experts, criminals, and other civilians for their military efforts.[13]

While Russian cyber threat activities related to the war in Ukraine have focused predominantly on Ukrainian targets, several incidents have spilled over to other countries, posing threats to the international community.[14] One example is the operation by Russian cyber threat actors on February 24, 2022, that disrupted most of Viasat's European KA-SAT satellite communications service network, although initially only targeting the Ukrainian military's communications

[8] Hansika Saxena and Aastha Mittal, Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022, in: CloudSek, 2022, p.1, https://cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022 (accessed April 10, 2023).
[9] Ashish Khaitan, "US Cyber Attacks 2023: Cybercrime has Caused an Estimated $6 Trillion in Damages in 2022 Alone," in: The Cyber Express, March 23, 2023, https://thecyberexpress.com/us-cyber-attacks-2023-trends/#:~:text=The%20United%20States%2C%20Saudi%20Arabia,primary%20source%20of%20digital%20malfeasance, (accessed April 10, 2023).
[10] Check Point Research, 2023 CYBER SECURITY REPORT, 2023, p. 20, https://pages.checkpoint.com/cyber-security-report-2023.html (accessed April 10, 2023).
[11] ENISA, ENISA Threat Landscape 2022, 2022, p. 4, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends (accessed April 10, 2023).
[12] Google, Fog of War How the Ukraine Conflict Transformed the Cyber Threat Landscape, 2023, P. 7, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf (accessed April 10, 2023).
[13] Check Point Research, 2023 CYBER SECURITY REPORT, 2023, p. 20, https://pages.checkpoint.com/cyber-security-report-2023.html (accessed April 10, 2023).
[14] Canadian Centre for Cyber Security, Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine, 2022, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine (accessed April 10, 2023).

capability. On March 10, thousands of KA-SAT satellite modems were out of service as a result, among them modems in France, Germany, Greece, Hungary, Italy, and Poland.[15]

As a consequence, experts expect to see more geopolitically motivated cyber operations against governments in the near to medium term. A study published by CloudSek shows that the government sector has emerged as a prime target for cybercriminals in 2022. The study finds that hacktivist activity accounted for about nine percent of the recorded incidents in the government sector. Six percent of all reported incidents were attributed to ransomware groups. The number of government-sponsored attacks also increased. This growth is primarily due to the emergence of new cyber threat actors (CTAs) such as Initial Access Brokers (IABs) and criminal activities such as Ransomware-as-a-Service (RaaS).[16] IABs are cybercriminals that sell access to compromised networks. Through RaaS, cyber criminals do not necessarily need to have the technical skills themselves to create corresponding malware.

Besides the growing geopolitical importance of cyber threats, emerging and disruptive technologies (EDTs) such as artificial intelligence (AI) powered models as well as the growing availability of data have extended the scope of attacks and the level of damage.[17] On the one hand, technologies like AI can be utilized to better detect threats and protect systems and data resources. On the other hand, AI can be used to detect patterns in computer systems that reveal vulnerabilities in software, or to develop malware that is constantly changing to avoid detection by automated defensive tools.[18] The proliferation of AI-based models has not only reduced the costs of cyberattacks but also amplified their speed and sophistication. In the coming years, organizations must increasingly balance the value of new technologies and the potential cyber exposure that comes with them.[19]

What are the top cyber security risks in 2023? While some of them are new, others have dominated the list of top cyber risks for years. According to several studies, these include phishing and smishing, malware, ransomware (and Ransomware as a service), business e-mail compromise, trusted insider threats, unintentional disclosure, storage reconnaissance (unprotected cloud storage), zero day attacks, social engineering, data exfiltration, human error and poor cyber hygiene, cyber-physical attacks, state-sponsored attacks, and IoT attacks.[20] Another problem often identified is a severe shortage of cybersecurity professionals. Within its Threat Horizon study, the

[15] Canadian Centre for Cyber Security, Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine, 2022, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine (accessed April 10, 2023).
[16] Hansika Saxena and Aastha Mittal, Unprecedented Increase in Cyberattacks Targeting Government Entities in 2022, in: CloudSek, 2022, p. 4, https://cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022 (accessed April 10, 2023).
[17] World Economic Forum, Global Cybersecurity Outlook 2023, Insight Report, January 2023, p. 3, https://www.weforum.org/reports/global-cybersecurity-outlook-2023/ (accessed April 10, 2023).
[18] Bob Violino, Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most, in: CNBC, April 12, 2022, https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html (accessed April 10, 2023).
[19] World Economic Forum, The Global Risks Report 2023, 18th Edition, 2023, p. 8, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (accessed April 10, 2023).
[20] BDO Digital, Top 10 Cyber Security Threats to Businesses in 2023, December 2023, https://www.bdodigital.com/insights/cybersecurity/top-10-cybersecurity-threats-to-businesses-in-2023 (accessed April 10, 2023).

Information Security Forum, identifies "three Ds of cyber threats": disruption, distortions, deterioration. Thus, the organization expects that over-reliance on fragile connectivity creates the potential for premeditated internet outages, with severe consequences to the economy but also to public services (disruption). The spreading disinformation environment is likely to compromise trust in the integrity of information (distortion), while rapid advances in intelligent technologies plus national security concerns and privacy regulations impact organizations' ability to control their own information (deterioration).[21]

Who is in charge when it comes to the manifold dimensions of cyber security? The lines of responsibility between national and international actors as well as the civilian and military space are blurry and deeply affected by the lack of skilled workers and a rapidly changing cyber landscape. It is clear that fighting cybercrime requires a multi-stakeholder approach, since cyberattacks do not stop at borders, sectors, or entities and have the potential to impact individuals, organizations, countries, and the global order simultaneously.[22]

Against this background, the 10th Munich Cyber Security Conference (MCSC), titled "Cyber Security: Who is in Charge? – Dealing with Blurred Lines of Responsibility" brought together more than 40 high-level speakers and several hundred selected guests from Europe, North America, Africa, and Asia. Together they discussed different lines of responsibility, how to find a better understanding in interlinking them, as well as how military conflict can affect non-military targets.

KEY TAKEAWAYS

1. Changing Threat Landscape Driven by Geopolitical Tensions

Advancing digitalization and the increasing dependence of societies on it in all areas of life go hand in hand with an evolving cyber risk landscape and the increasing danger of cyberattacks. The Russian invasion of Ukraine has shown that digital technologies have become a potent weapon of war. Cyber actors conduct operations that are coordinated with kinetic military actions. Hacktivist groups are choosing sides, some being contracted by governments, some acting independently. Disinformation campaigns also belong to the warfare toolkit. Civilian organizations and businesses such as social media platforms and media also play a growing role in the means of war.

Due to growing geopolitical tensions worldwide, the number and magnitude of disruptive cyber operations are likely to grow in the near- to mid-term future. A key driver is the growing systemic conflict between autocratic and democratic countries, especially China and many countries of the West, foremost the United States. In this context, experts warn that the risk of China invading Taiwan is growing. The consequences would be of even greater magnitude than the Russian war in Ukraine. The cyber sector would likely play a major role in such an attack.

[21] Michelle Moore, Top Cybersecurity Threats in 2023, University of San Diego, https://onlinedegrees.sandiego.edu/top-cyber-security-threats/ (accessed April 10, 2023).
[22] Larisa Redins Cybersecurity: Who is responsible?, Cybersecurity Guide, March 27, 2023, https://cybersecurityguide.org/resources/cybersecurity-responsibility/ (accessed April 10, 2023).

2. Cyber Defense is the New Offense

Russia's invasion of Ukraine has led to a range of specific learnings concerning cyber space. For one, the destructive power of cyber offense has generally been overestimated, as Russia's cyberattacks on Ukraine have remained largely unsuccessful and have not given Russia a fundamental advantage in the war. This should not lead to complacency, however. In principle, cyberattacks and disinformation campaigns have massive disruptive power. But the risk can be reduced by having well-functioning defense strategies and systems in place. This leads to a second learning. Reacting to an attack, when it happens, is often too late. Rather, cyber resilience of individuals and organizations, i.e., "the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack" (European Central Bank), is decisive in reducing the risk of cyberattacks and disinformation campaigns and countering them in the event that they do take place. Building cyber resilience is not done overnight but instead requires a long-term strategy and a multi-stakeholder approach. Governments, companies, and civil society organizations need to invest in the abilities of the people operating technologies, including capacity building and training. Moreover, increased public-private partnerships as well as international cooperation are needed.

3. No Cyber Resilience without Public Private Partnerships

Russia's war against Ukraine underscores the centrality of public-private partnerships to a holistic approach to cyber security. As such, the Ukrainian defense strategy demonstrates that a broad alliance of actors has managed to accelerate capabilities and share information rapidly, thereby enhancing Ukraine's cyber defenses and promoting its resilience. This example underlines the systemic power of liberal democracies and their multi-stakeholder approaches, as opposed to the autocratic system of centralizing all actions under the government. While some experts use this example to argue for a decentralization of government systems and a distribution between public and private actors, others warn against taking this too far. Especially in the field of digital infrastructure, the dependence on private actors could also lead to vulnerabilities. In this context, many caution to take a closer look at the ownership structure of critical infrastructure, calling for more assertive screening of foreign direct investment. A recent example is the involvement of Chinese companies in Western 5G networks. In sum, governments need to scrutinize in which areas decentralization between public and private actors could be beneficial to building cyber resilience and in which it could lead to greater vulnerabilities. One answer could be the creation of public-private emergency response teams ready to deploy when needed.

While public-private partnerships are without doubt necessary to build cyber resilience, they are complicated. Not only are there unclear responsibilities between actors, but there is also a lack of trust between government agencies and companies. As such, Western governments often have high expectations and demands on private companies, while the private sector considers them unworkable and expects the government to create and enforce an appropriate framework and rules-based order. One useful step toward deepening understanding between the two sides is the

implementation of advisory councils composed of private sector executives to make actionable recommendations to the government. Overall, there needs to be a fundamental recognition that both the public and private sectors are on the same team.

4. Capacity Building for Cyber Resilience

A key component of successfully strengthening cyber resilience is closing the capacity gap in the cyber sector. This means building functioning and accountable institutions to respond effectively to cyber crime and to strengthen a country's cyber resilience. The need for cyber capacity building arises from the growing complexity and sophistication of cyber threats as well as the increasing reliance on digital technologies across various sectors. It is essential to build robust cyber capabilities at the individual, organizational and national levels to effectively address these challenges.

One key aspect is meeting the soaring demand for skilled cybersecurity professionals by providing adequate training and retaining talent in the sector. Cybersecurity Ventures (2022) projected a 350 percent increase in global cybersecurity job openings by 2025, reaching 3.5 million total open jobs. Many national and international initiatives are already in progress to address this need. For instance, the EU Commission established the Cybersecurity Skills Academy in April 2023, while the German Cyber Security Strategy (2021) aims to foster IT security research in schools and universities. An example from the private sector is Microsoft, which is collaborating with U.S. community colleges to skill and recruit 250,000 individuals into the cybersecurity workforce by 2025. Given the high demand for cyber professionals and the rising threat landscape, it is imperative to sustain and intensify these efforts.

Furthermore, in the face of an ever-evolving cyber landscape, continuous review and adaptation of national and international policy and legal frameworks are necessary to remain up to date. Moreover, fostering values-based international cooperation and collaboration among nations, organizations, and stakeholders is vital to share best practices, exchange information, and collectively address global cyber threats. Other aspects of cyber capacity building should involve increasing public awareness of cyber threats, enhancing technical infrastructure, and bolstering the cyber resilience of organizations.

5. International Cooperation is Key to Cyber Resilience

Cyberattacks have no regard for national borders, as they can quickly spread across sectors and countries via global supply chains, while the perpetrators can operate from anywhere in the world. To effectively combat cybercrime, national institutions must enhance cooperation with their counterparts in other countries, both bilaterally and multilaterally. This necessitates the establishment of improved channels of communication to facilitate faster data exchange, more effective identification of vulnerabilities, and the development of joint action plans. Moreover, it is crucial to strengthen the interface between law enforcement and the private sector. The global community must intensify its efforts to find values-based solutions in response to the evolving threat landscape, with mutual trust, shared rules, and perspectives serving as key factors for meaningful cooperation.

As the systemic competition between autocratic and democratic countries grows, special focus should be laid on new ways of cooperating with the Global South on cyber and enhancing trustful cooperation. Additionally, it is pivotal to further strengthen cooperation between the European Union (EU) and the United States. In 2021, the transatlantic partners launched the Trade and Technology Council (TTC), which includes dedicated working groups focused on coordinating information and communications technology (ICT) and data governance. Given recently adopted and emerging legislation on both sides of the Atlantic, such as the Strengthening American Cybersecurity Act of 2022 and the European Cyber Resilience Act introduced in 2022, it is essential for the EU and the United States to ensure that cyber security standards, reporting requirements, and subsequent cyber threat assessments do not diverge further. By aligning their efforts, cooperation between the EU, the United States and other allied nations can be an essential competitive advantage.

Conference Day 1

Welcome

Claudia Eckert, *Chairwoman of Security Network Munich & Executive Director of Fraunhofer AISEC (Munich)*

During her opening statement, Claudia Eckert reflected on the 9th edition of the Munich Cyber Security Conference. Looking back a year ago, participants were hopeful about resolving the conflict that eventually led to Russia's invasion of Ukraine. Today, the war presented unprecedented risks comparable to those witnessed during the era of the Iron Curtain. Claudia Eckert emphasized that the Russian aggression had profoundly unsettled the foundations of Europe and the global order as a whole.

Expanding on the conference theme, "Cybersecurity: Who is in charge?", she explained that it encompassed not only delineating various lines of responsibility and establishing better cooperation to enhance efficiency in addressing cyber risks. It also acknowledged the reality that

cyberspace was interconnected, meaning a military conflict could have repercussions beyond purely military targets.

In light of these circumstances, Claudia Eckert concluded that it was imperative to reevaluate defense mechanisms and strategies, integrating them to respond to the current geopolitical developments effectively. She valued the MCSC as a platform for experts to engage in this critical thinking process, facilitating mutual understanding and collaboration among organizations and countries.

Opening Keynote

Judith Gerlach, *Bavaria's State Minister of Digital Affairs (Munich)*

In her opening keynote, Judith Gerlach reflected on the latest developments in the cyber threat landscape. She began her statement with a timely case: ChatGPT, the AI-driven chat bot that is making headlines for its ability to process natural language and generate human-like text based on the input it is given. According to Judith Gerlach, this example perfectly showcased the new realities society must face regarding AI. Technological progress had created nearly endless new possibilities, with ramifications for the daily lives of individuals, businesses, and societies. After underlining the positive potential of these technological advancements, Judith Gerlach also acknowledged the need to critically consider the threats as well dangers to democracy. As such, she warned that the use of AI and automation in information ecosystems could "create fake news on steroids." She argued that it was like a hammer: "You can build a house with it, or you can smash a window." This message circled back to the conference's theme: the role and sharing of responsibility. In this regard, Judith Gerlach called for a holistic approach to cyber risks and emergencies.

Subsequently, she touched upon the geopolitical dimensions of cyber security, pointing at the systemic rivalry between the United States and China and their competition for domination over new technology such as AI. Judith Gerlach urged democracies to step up their efforts in the arms race for leadership in the technology and cyber domain. In order to do so, she emphasized that Germany needed to cultivate partnerships and alliances to have access to and enable the development of key technologies to not lose this international competition.

Conference Day 1, Fireside Chat

Kemba Walden, *Acting National Cyber Director in the Executive Office of the U.S. President (Washington D.C.)*

Christopher Krebs, *Founding Partner of the Krebs Stamos Group (Washington D.C.)*

On her first day in office as the Acting National Cyber Director, Kemba Walden sat down with Chris Krebs to discuss her take on the current cyber security landscape, her analysis of recent developments and trends, and her priorities and goals for the time ahead.

Regarding the forthcoming U.S. National Cybersecurity Strategy, Kemba Walden emphasized three focal areas: Shifting responsibilities, investing in resilience, and being proactive. First, she underlined that a shift of responsibility for cyber security risks was needed. This included shifting the responsibility from end users more to producers as well as from the state and local level to the federal government. Second, a cyber security strategy would have to incentivize investment in order to establish reliability and resilience. Kemba Walden further mentioned the importance of harmonizing regulations and focusing on regulating the parts of industry that were currently unregulated. This would allow national cyber security initiatives to get ahead of adversaries. Third, the strategy should have a proactive character. Christopher Krebs agreed with Kemba Walden, pointing out that the national threat landscape had changed fundamentally, and that the government needed a new, more effective strategy. To illustrate this, he referenced the Colonial Pipeline Hack.

Kemba Walden then emphasized that the Russian war against Ukraine had led to a reassessment of the role of cyberspace in the geopolitical context. She shared three key lessons regarding the role of cyber: First, the conflict demonstrated a substantial shift away from the analytical status quo that viewed cyber as a domain that substantially favored the attacker. Instead, Russia's war against Ukraine had showcased the increased role of cyber defense. "In cyber, defense has become the new offense," she underlined, meaning that it was no longer just about preventing a cyber security attack when it happened but instead about focusing on capacity building and training while anticipating a potential attack. Second, cyber offense was incredibly difficult. In fact, experts had overestimated Russia's ability to keep up the cyber offensive. Third, Kemba Walden stressed that Ukraine's handling of the cyber space showed the power of narratives and, in turn, that people were still more important than technology. Considering the increasingly conflictual international environment, Kemba Walden looked ahead and shared advice to prepare for a changing threat landscape: First, investment in the abilities of the people operating technologies was needed, to include capacity building and training. Second, the responsibility should not be laid solely on the government but had to include contributions from the private sector. Third, she stressed to never underestimate the importance of a proper defense.

Looking at these developments, Kemba Walden emphasized that international cooperation on cyber security was urgently needed. She highlighted that digital ecosystems were dependent on one another; in times of almost total interconnectedness, one was only as strong as the other. Therefore, problems were not entirely unique, even across industries. That said, international partners needed to work on identifying common problems to formulate common solutions.

Conference Day 1, First Panel

Cybersecurity – Who is in Charge? Managing Different Lines of Responsibility

Moderator**: Ciaran Martin,** *Professor at University of Oxford and Former Director of the UK's National Cyber Security Centre (Oxford)*

Despina Spanou, *Head of Cabinet for European Commission Vice President Margaritis Schinas (Brussels)*

Andreas Könen, *Director General for Cyber and Information Security at the Federal Ministry of the Interior and Community (Berlin)*

Kai Horten, *Partner at AltoPartners Germany (Munich)*

Robert Strayer, *Executive Vice President of Policy at the Information Technology Industry Council (Washington D.C.)*

On the first panel, representatives from the German government, the EU Commission, and the private sector came together to share their perspectives on the question of who holds primary responsibility for cyber security.

First, the panelists agreed that governments should set the framework conditions for today's cyber security environment. In this context, Kai Horten emphasized that the blurred jurisdictional boundaries that currently characterize the cyber ecosystem were not sufficient. "Cyber security is like team sports and like in many sports, you better train and rehearse what people need to do across the organization," he stated. The private sector expected the government to construct and enforce a proper framework and rules-based order. Despina Spanou underlined that the European Commission was committed to taking on that role.

Driven by the goal of improving European security, the EU has been continuously implementing and adapting its regulation of cyber space. According to Despina Spanou, this could be viewed as a three-level process. On the first level, in 2016, the EU had improved cyber resilience through Directive (EU) 2016/1148 (known as NIS directive) by addressing critical infrastructures and establishing common rules, oversight, and preventive measures. On the second level, in 2022, the EU had passed the Directive (EU) 2022/2464 (known as NIS 2 directive), encompassing building on lessons learned and broadening the scope of the measures beyond the traditional sectors. On the third level, Despina Spanou highlighted the importance of security-by-design, requiring products and services circulating the market to fulfill cyber security standards. This could only be done by closing the cyber professional's gap. The EU wanted to contribute to this, for example, through the soon-to-be-opened Cyber Security Skills Academy.

Andreas Könen underlined that the German government appreciated the cooperation and involvement of the EU and agreed that the EU played an important role as rule setter. Nevertheless, he emphasized that national governments were still the ones responsible for implementing the rules. On that note, Robert Strayer urged the audience to recognize the cross-border nature of cyber resilience and argued for an international – instead of regional – harmonization of rules in order to

prevent the fragmentation of markets. The United States aimed to play a leadership role in this. This was received well by the European representatives on the panel, who appreciated that the transatlantic relationship had changed significantly for the better, with promising cooperation and approaches beginning to align.

Subsequently, the discussants focused on the relationship between governments and the private sector. Andreas Könen outlined the different responsibilities. According to him, the business sector, for example, had to implement security-by-design approaches and hire qualified experts to improve cyber security. The role of the government, on the other hand, was to manage the cyber threat landscape and provide specific advice to companies on its nature and evolution. Looking at the United States, Robert Strayer described that the U.S. government had made a shift in its approach, becoming more actively involved in corporate cyber resilience than in the past and was planning to introduce more regulation and regulatory oversight. He emphasized that this could only be successful in conjunction with close collaboration with the private sector to meet the needs of businesses and not create further burdens.

Ultimately, all panelists agreed that more robust cooperation between government and the private sector was needed. Looking ahead, they identified important pillars of improved cyber resilience including more speed and efficiency, more redundancy in some structures and less in others, less stand-alone strategies by governments, a clearer definition of priorities, as well as less strategizing and more implementation.

Conference Day 1, Fireside Chat

Margaritis Schinas, *EU Commission, Vice President (Brussels)*

Ralf Wintergerst, *Group CEO, Giesecke+Devrient (Munich)*

In a fireside chat with Ralf Wintergerst, Margaritis Schinas argued that cybersecurity had to be a joint effort among like-minded partners. First and foremost, the European Commission set forth a holistic approach to cyber security. Achieving transformative changes in pursuit of multiple goals was only possible in a team effort. In this context, the Commission emphasized the need to leverage the benefits of "Team Europe," which had been demonstrated in the successful fight against the COVID 19 pandemic. Overall, the regulatory landscape at the European level was taking shape. At the same time, he cautioned the EU Commission not to go-it-alone in cybersecurity regulation, but instead as "Team Europe that brings together institutions, member states, agencies, and industries". Furthermore, cyber regulation required international cooperation with other international allies and partners, the "Team West". According to Margaritis Schinas, all stakeholders had to work together and do their part. In this regard, he advocated for the establishment of emergency teams, which were ready to act when needed. These needed to include trusted experts from the private sector. Emphasizing the importance of cooperation with the private

sector, he touched upon a challenge, which both governments and the private sector faced: a lack of skilled personnel. Therefore, continuous training and capacity building were essential.

Looking outside of Europe, Margaritis Schinas acknowledged the global race for tech leadership and the ramifications this had for the European market as well as its security infrastructure. Being outspent globally on new technologies, the EU had to find a way to enable more investment in innovation in cyber and tech. Altogether, the only way forward as Team Europe was to utilize all resources, power, and skills.

Conference Day 1, Impulse

Sir Alex Younger, *Former Chief of Secret Intelligence Service MI6 (London)*

In his keynote address, Sir Alex Younger pointed out a key problem of the digital and cyber domains: "the internet, albeit our invention, was not on our side". The general assumption that technology would work automatically and always to peoples' benefit had proven to be false, according to him. In fact, technology could be bent to the purposes of societal control, the effects of which were showcased by the rise of digital authoritarianism. This led to a key question for this generation: Which value system would be the default setting for the Internet? In other words, would the benefits or the dangers of technology determine the course of the digital age? For the former Chief of MI6, this came down to teamwork – within bureaucracies, between the public and the private sector, as well as between global partners.

Sir Alex Younger underlined that teamwork was one of the main advantages the West had over its systemic rivals, hence, it should double down on its efforts. The West was strongest, if it stood true to its liberal democratic principles: "Beat the Russians, don't be the Russians", Sir Alex Younger argued, alluding to practices in the digital and cyber sphere. One of these principles was that of decentralization. Hence, Western governments should always leverage distributive systems that brought the power of public and private actors together. Extending this learning to China, arguably the main geopolitical competitor of Western democracies, Sir Alex Younger stated that China would win in any domain that was centralized, whilst the West would win in any that was decentralized.

Conference Day 1, Second Panel

Dual Use: Merging Defenses in Cyber – The Way Forward?

Moderator: **Alexander Schellong**, *Vice President Cybersecurity at Schwarz Group (Munich)*

Mieke Eoyang, *Deputy Assistant Secretary of Defense for Cyber Policy at U.S. Department of Defense (Washington D.C.)*

Sandra Joyce, *Vice President at Mandiant Intelligence (Washington D.C.)*

Alix Carmona, *Vice President and Head of Cyber Programmes at Airbus Defense and Space (Munich)*

Robert Koch, *General Staff Officer of the Federal Armed Forces (Munich)*

During the second panel of the conference, the discussants took a closer look at cyber in today's security and defense infrastructure. Nearing its one-year mark, the war in Ukraine provided valuable learnings and takeaways in this regard. Mieke Eoyang perceived Russia's cyber offensive to be less powerful than anticipated; rather it was the defense that turned out to be the differentiator. While generally agreeing, Sandra Joyce contested that it would always remain easier to find the one hole in the system than to defend it. However, the important thing was to learn from it and to be better prepared the next time around. Another learning regarding Ukraine was the importance of the private sector in cyber defense. Sandra Joyce doubled down on this point, arguing that the private sector's assistance to Ukraine on cyber defense showcased the power of the industry. Looking at the intersection of civilian and military applications, Alix Carmona also identified great value in cooperation between governments and the private sector but prescribed a more effective sharing of learnings and takeaways.

Robert Koch shared the military's perspective, outlining the capacities, capabilities, as well as legal limits of the defense sector. He also raised the question of whether modern digital technologies made the military stronger or more vulnerable. To cope with vulnerabilities, the military could improve its applications through cooperation with the industry and a strengthening of the military-industrial base. He concluded that better cooperation also needed to extend to the international realm.

Picking up on this line of thought, the panelists discussed international cooperation, cautioning the differing views on cybersecurity between the transatlantic partners. Sandra Joyce commented on the different narratives in the United States and the EU. In the United States, "cyber security is about bad actors doing bad things to good people. In contrast, in Europe, it is about regulation and standardization. In the end however, both mindsets together are important for cyber security", she underlined. This gap in mindsets and approaches had to be bridged in order to unlock the full potential of cooperation in cyber defense.

In conclusion, the panelists agreed on three key takeaways: First, national approaches had to be aligned more between international partners. Second, military and civilian actors had to double down on their efforts to cooperate more closely. Third, the capacity and capability gap had to be closed both in the government and the private sector. This included, first and foremost, to increase investment in skills and lifelong learning.

Conference Day 1, Spot On

Looking Beyond - Other Dimensions of Cyber

Moderator: **Gregor P. Schmitz**, *Editor-in-chief at Stern Magazine (Hamburg)*

Sabine von der Recke, *Member of the Management Board at OHB System AG* (Bremen)

Philip Venables, *Vice President and Chief Information Security Officer, Google Cloud (Mountain View)*

Christopher Ahlberg, *CEO of Recorded Future (Washington D.C.)*

The spot-on discussion brought together three distinct viewpoints to cover different dimensions of cyber, such as in space-based infrastructure, defense, and AI. Phil Venables opened the discussion by giving an assessment of the state of the global cyber situation. He summarized his perception as pessimistic in the short-term, alluding to the omnipresence of cyber-attacks. At the same time, he also stated to be a long-term optimist, as the sophistication of defense mechanisms and resilience improved and imposed higher costs on attackers. Sabine von der Recke underlined this ambivalent assessment with the concrete example of space-based infrastructure and its role in Russia's war on Ukraine. On the one hand, the Russian cyber-attack targeting the American commercial satellite internet company Viasat showed how vulnerable this infrastructure was. On the other hand, the Ukrainian use of the satellite network Starlink offered a huge advantage to the Ukrainian armed forces and showed how important this infrastructure was to communication. She added that the Russian invasion led to the realization that agreed-upon treaties, like the Outer Space Treaty, may no longer be considered binding by all sides. Therefore, policymakers had to consider how to secure the space infrastructure in space as well as on the ground. Here, Phil Venables pointed to the need for increased public-private and private-private partnership. He emphasized that this cooperation could only succeed if it was embedded in the DNA of all stakeholders. Christopher Ahlberg, however, voiced his doubts about the feasibility of public-private information-sharing and proposed that intermediary actors could take ownership of the problems at hand.

The discussion then pivoted to the AI dimension of cyber, and the panelists asked whether its rise was a threat or an opportunity. For Phil Venables, the important point to understand was that AI was not at all a new technique, "it is already deeply embedded in every sector around the world." He continued underlining that AI had proven highly advantageous for cyber defense. Christopher Ahlberg added a concrete example of an AI-run intelligence dome, which his company and the Ukrainian government successfully built to defend against the Russian military. According to him, the technical advantage of AI was impossible to match by humans.

In essence, all panelists agreed that the goal should be the responsible, safe, and ethical use of AI, which centered around the consequences of its application.

Conference Day 1, World View

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

In his input statement, Japanese representative Akihiro Wada shared his Japanese and Far East perspective on cyber security issues. According to Akihiro Wada, the approach of the Japanese Business Community to cyber security was built on three pillars: The first was cross-industry cooperation that included the entirety of a supply chain. The second was international cooperation and the third was public-private partnerships. "We believe in cyber security for all and cyber security by all," he stated, in reference to the conference's main question of who is in charge. This overall strategy seemed to be aligned with the basic principles and priorities of U.S. and European approaches. He warned that the cyber threat level was continuously increasing, with attacks around the Tokyo Olympics at an all-time high. In Japan, cyberattacks were now understood as national security risks. In consequence, Japan published its Cybersecurity Declaration, outlining key parameters of its strategy. These included enhancing cyber security for the entire supply chain and the importance of public-private partnerships. Looking ahead, Akihiro Wada explored the potential for cooperation and partnerships that included increased dialogue with likeminded countries with the sharing of threat perceptions and best practices.

Conference Day 1, Third Panel

Name of the Game: Teamplay – Overcoming Cyber Gaps

Moderator: **Geoff Brown**, *Vice President at Recorded Future and Former CISO New York City (New York)*

Erkki Lego, *Director of EU CyberNet at the Estonian Information System Authority (Tallinn)*

Thomas Boué, *Director General for Policy at BSA | The Software Alliance (Brussels)*

Thomas Rosteck, *Division President Connected Secure Systems at Infineon (Munich)*

Jessica Keiser, *Vice President Cyber Defense Center at Bayer AG (Leverkusen)*

The third panel of the conference discussed whether current formats of cooperation and alliances in cyber were merely terms used on paper or filled with operational substance. One example of productive, trusting and effective teamplay was the EU Commission Initiative for Cyber Capacity Building, according to Erkki Lego. He said this initiative brought together cross-border stakeholders in regular meetings under Chatham House rules to share best practices and exchange views. Furthermore, the work of the CSSA, an alliance of companies jointly facing cyber security challenges, showed how frequently and productively business engaged in information-sharing.

In comparison, the existing formats for cooperation also demonstrated a lack of trust between government agencies and companies, Jessica Keiser explained. Even though the private sector relied on the public sector for provision of services, the blurred lines of responsibility made it difficult to form a sustainable and trusting partnership. The panel dove deeper on this point, and

the panelists explained their perspectives on how this lack of clarity played out operationally. According to them, the sheer number of different governmental agencies and their individual requests to private actors lead to an enormous amount of additional work. Accordingly, policies often did not fit the operational needs.

From an industry perspective, there should be better cooperation between public and private actors in the field of standardization and regulation, according to Thomas Rosteck. Regulators needed to establish an industry-wide, level playing field. In order to achieve meaningful teamplay, Thomas Boué urged both the public and the private sectors to realize that they were on the same team and shared similar objectives.

Thomas Rosteck stressed that policymakers needed to ensure that the world did not become more fragmented. A pursuit of uniformity in the regulatory frameworks by likeminded partners could eventually lead to improved interoperability of industry products. Thomas Boué reiterated this point, stating " instead of saying that we have a competitive advantage in certain aspects, we should strive to show that industry and government are like-minded." On the industry side, a security mindset regarding cyber was needed. Companies needed to move away from cyber departments operating in silos towards creating awareness for a shared responsibility throughout all operations. On the societal level, digital literacy and cyber competencies needed to be established early so that individuals no longer viewed cyber as an expert issue but better understood their role and possible contributions to decrease risks and increase resilience.

Conference Day 2, Keynote

Catherine De Bolle, *Executive Director of Europol (The Hague)*

Oliver Rolofs, *Founder and Managing Partner of COMMVISORY (Munich)*

In her keynote, Catherine De Bolle outlined how Europol contributes to the fight against cybercrime and explained the manyfold challenges. Looking at the overall landscape of cybercrime, Catherine De Bolle attested that both the volume and the sophistication of cyberattacks were increasing, causing major losses for governments, businesses, and individuals. The law enforcement agencies had to continuously reinvent themselves and find creative approaches to counter the methods of cyber criminals. Three key features came together to create the motive and the opportunity for cyber criminals: First, the overall digital environment, which enabled actors to operate anonymously; second, the spread and accessibility of anonymous payments; and third, that data could quickly and easily be leveraged for financial gains. Catherine De Bolle underlined that "data is the new gold, and with data you have the ability to ask for money."

Next, Catherine De Bolle pointed out that cyber criminals were very calculated in their actions and operated in an economic way. Hence, they targeted vulnerabilities. Small and medium-sized enterprises (SMEs) were often victims due to their insufficient cyber security mechanisms. Sketching how these types of cybercrime could be combatted, Catherine De Bolle underlined the importance of cross-border team efforts that encapsulated the sharing of information and cooperation between law enforcement agencies as well as industry, academia, and the cyber security community. All actors had complementary roles to play; the challenge was the definition of those roles. This had become especially significant in light of the increasingly blurred lines between defense, law enforcement, and civilian cyber security competences. Every actor needed to reflect on its role and contribution in the effort to create a secure digital environment for citizens and businesses.

Finally, outlining Europol's steps to become future proof in its fight against cybercrime, Catherine De Bolle highlighted the efforts to stay on pace with the criminals. This entailed investments in new tools, skills, and expertise for law enforcement and justice communities.

Conference Day 2, Fourth Panel

Talking about Resilience

Moderator: **Jannis Brühl,** *Süddeutsche Zeitung (Munich)*

David Wolpoff, *Chief Technology Officer of Randori (Denver)*

Mikko Karikytö, *Chief Product Security Officer & Head of Product Security at Ericsson (Helsinki)*

Srdan Dzombeta, *Partner at EY (Berlin)*

Nicholas Leiserson, *Assistant National Cyber Director for Cyber Policy & Programs (Washington D.C.)*

During this panel, the discussants agreed that there was no single silver bullet to improve cyber resilience. Rather, it encompassed different components and required varied strategies. Cyber resilience was understood as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, attacks, or compromises on systems that use or are enabled by cyber resources.

Nicholas Leiserson explained that cyber resilience was a moving target as the threat landscape changed continuously, arguing for a multistakeholder approach. Improving cyber resilience required, first and foremost, flexibility and awareness. For the private sector, this encompassed a transformative process, as every company, no matter the size or sector, had to face the realities of the threat cybercrime presented. Srdan Dzombeta built on this, making the point that organizations needed to be more flexible to be truly resilient. More specifically, he urged organizations to approach their security infrastructure through the eyes of the attacker. At the same time, he cautioned that it would never be possible to disarm an attacker entirely because they could utilize new technologies more easily.

Nicholas Leiserson referenced the conference title "who is in charge?" and stated that "making sure people understood where the responsibly lies, across the private and public sector is critical in order to get cyber security resilience correct."

The panelists also discussed whether governments had sufficiently assisted companies to improve cyber resilience. Mikko Karikytö pointed out that global businesses desired a global set of rules and standards to be better able to cope with the new realities and make operations easier and more predictable. Further, governments were called on to enforce their rules more effectively. Internationally, this required cooperation to pressure states that did not adequately pursue cyber litigation.

Fundamentally, the panel agreed that resilience was a work in progress. Rather than seeing security as an absolute, it was more important to internalize resilience as a mindset. Lastly, they underlined that the private and public sector both had responsibilities to improve resilience, as they each had specific areas in which they were better equipped.

Conference Day 2, Vantage Point

Investment Security

Paul Rosen, *Assistant Secretary of the Treasury for Investment Security (Washington D.C.)*

In his talk, Paul Rosen took stock of how data and cyber factored into the national security risk assessment of foreign direct investment (FDI) into the United States. The general task was in the balance of facilitating FDI, while mitigating any security risks that went along with the investment. Paul Rosen underlined that the United States was committed to openness to foreign investment as this was a cornerstone for economic growth and helped to maintain the economic and technological edge of the country. At the same time, he stressed that investments of certain persons and businesses, particularly those from adversarial nations, could present risks to U.S. national security. The United States therefore conducted a careful investment screening.

At that center of this process stood the Committee on Foreign Investment in the United States (CFIUS). Paul Rosen explained that the investment screening process had repeatedly been modernized and tightened in recent years, both through legislation and presidential executive orders. He explained that CFIUS played an important role in the overall national security priorities of the Biden Administration, which prioritized preserving U.S. technological leadership, protecting sensitive data of American citizens, and enhancing U.S. supply chain resilience. Paul Rosen also mentioned that President Biden had mandated CFIUS per executive order to consider several new national security factors during its review process. Among them were cybersecurity risks that threaten to impair national security. As such, CFIUS was to review whether an investment might provide a foreign person with the ability to conduct cyber intrusions or other malicious cyber-enabled activities that pose a risk to national security.

Cyber and data created novel challenges in this undertaking and necessitated a sound risk and vulnerability analysis. This included an investigation of what exactly was being acquired by a

foreign company, as there was a shift away from traditional acquisitions. That analysis had to be much more sophisticated and thorough due to the complexities of data. Paul Rosen explained that data could be weaponized. As such, special scrutiny was called for when U.S. personal data was involved. He also underlined that close cooperation with international allies was needed. This involved similar standards in investment screening as well as an exchange of information.

Talking Heads

Cybercrime: Lines of Action

Moderator: **Marc Raimondi**, *Chief of Staff at Silverado Policy Accelerator (Washington D.C.)*

John P. Carlin, *Partner at Paul Weiss (Washington D.C.)*

Bryan Smith, *Section Chief for FBI's Cyber Criminal Operations Section (Washington D.C.)*

Nicholas Warner, *Advisor at SentinelOne (Boston)*

Valerie M. Cofield, *Chief Strategy Officer of the U.S. Cybersecurity and Infrastructure Security Agency (Washington D.C.)*

On this panel, experts in national security and cyber security discussed the issue of cybercrime, with a specific focus on ransomware. The panelists focused on two dimensions of current shortcomings in the defense against cybercrime. On the private sector side, an important vulnerability was the prevalent technology gap in both software and hardware that created opportunities for cyber criminals. On the government side, there was still a lack of effective cyber security legislation. Building on this, Valerie M. Cofield cautioned that the risks were particularly high for target-rich, but resource-poor actors, such as SMEs and state and local governments.

The panelists also discussed actions against cybercrime. Valerie M. Cofield cautioned that there was no way to truly eliminate cybercrime, but ways to make it harder and more expensive for criminals. As such, she pointed out proper cyber security hygiene, which, in her view, should be enforced more forcefully. John P. Carlin pointed out two lines of action focused on the role of government and the role of the victims. First, governments had to forcefully go after the criminals and significantly increase the costs of such crimes. Secondly, the victims had to be empowered by increasing their resilience across applications and sectors. Bryan Smith pointed out that effective law enforcement depended on victims reporting cybercrimes. However, many companies still shied away from reporting cybercrime incidents for fear of damaging their reputations.

Underlining that the fight against cybercrime required process, people, and technology, Bryan Smith detailed severe shortcomings, starting with the paucity of reporting by victims with only 20 percent of victims currently doing so. Secondly, he pointed at insufficient cooperation between companies and governments. He concluded by saying, "these systems are set in place to support our business needs, therefore, the business community needs to be more engaged to help solve this problem."

The panel also reiterated the importance of cooperating with international partners and pointed to recent successes of cross-border, international operations. In this context, a common solution needed to be found on how to deal with criminals who were being harbored or even supported by state actors, emphasizing the geopolitical dimension of cybercrime. Any solution needed to be viewed in light of the broader discussion of sustaining the global rules-based order in the digital age.

Conference Day 2, Impulse

Robert Silvers, *Under Secretary for Strategy, Policy and Plans at the U.S. Department of Homeland Security (Washington D.C.)*

In his impulse speech, Robert Silvers outlined the efforts of the United States to expand its international cyber security collaboration efforts.

In an era of cyber security, when cybercrime as well as nation-state cyberattacks quickly cut across national borders, international cooperation was more important than ever. Meetings and declarations were no longer enough: "We need transformational change in how we build cyber defense at the international level," Robert Silvers stated. An all-hands approach was needed that included coordination between the government and the private sector as well as between governments at the international level. He stressed that now was the time to really take the partnerships to the operational level.

Robert Silvers highlighted several multilateral initiatives, such as the Counter Ransomware Initiative, which brought together network defenders, law enforcement agencies, and financial regulators to combine efforts. Furthermore, he underlined the necessity of joining forces to protect critical infrastructure and network defense. In this regard, the U.S. collaboration with countries of the Middle East, such as Bahrain, the United Arab Emirates, and Morocco, was a prime example. In terms of like-minded partners such as the EU and the five Eyes Partners, the United States had established trustful connections for extensive intelligence sharing.

Transforming cyber defense at the international level was not only about how to collaborate today, but also about looking back and learning how to better defend against tomorrow's threats. Therefore, the United States had launched the Cyber Safety Review Board to conduct reviews of the most significant cyber incidents and publish recommendations for the community to learn and improve. Most notably, Robert Silvers mentioned the Cyber Safety Review Board's inaugural report of the log 4J vulnerabilities, which was one of the most significant software vulnerabilities affecting systems worldwide. The current threat environment demanded collaboration across borders, industries, and governments, to build a true architecture of security around the world's digital societies.

Conference Day 2, Fifth Panel

Geopolitical Dynamics: Tectonic Shifts in Cyber

Moderator: **David Lashway**, *Co-chair of Sidley Austin LLP (Washington D.C.)*

Dmitri Alperovitch, *Executive Chairman of Silverado Policy Accelerator & Co-Founder of CrowdStrike (Washington D.C.)*

Michael Rogers, *Former Commander of the U.S. Cyber Command and Director of National Security Agency (New York)*

Liesyl Franz, *Acting Deputy Assistant Secretary at the U.S. Department of State's Bureau of Cyberspace and Digital Policy (Washington D.C.)*

This panel took stock of current trends in the geopolitical landscape, including great-power conflicts, the potential return of zero-sum structures, and the attacks on states of the West and the liberal order. The panelists also assessed what role cyber played in this changing international environment. The panelists agreed that Russia's war against Ukraine marked a turning point in the European security order with great repercussions internationally. At the same time, the systemic rivalry between democratic and autocratic regimes was intensifying. The panelists also argued that the international system was becoming increasingly conflictual, and security threats more and more complex. They pointed out that the systemic conflict was especially salient in the digital sphere. In an increasingly digital economy, the liberal democratic order had to assert itself against autocratic digital rule. The panelists agreed that a combination of pressure and deterrence was necessary.

Dmitri Alperovitch argued that strong capabilities were key to maneuvering the new international risk environment. As in the case of Ukraine, building capabilities was a collaborative effort, in which partners had to pool their resources and operations. "Combined arms matter and cyber is one component of integration," Dmitri Alperovitch stated. To Michael Rogers, the Ukrainian defense efforts showcased that achieving substantial cyber resiliency was possible for those who were willing to pivot to different, more flexible models that integrate the government, the commercial world, and society. Several panelists pointed out that cyber resilience was not only technology-driven but that humans and their abilities were important differentiators.

On a positive note, Liesyl Franz argued that the widespread efforts to assist Ukraine indicated that the rules-based global order was very much alive. Nonetheless, threats were on the rise. First and foremost, the panel shared concerns over China's posture towards Taiwan and urged to avoid a conflict at all costs, as a war's ramifications would surpass those seen vis-à-vis Ukraine by a large magnitude. The key was to increase the leverage of the West over China, while simultaneously decreasing China's sphere of influence. Several of the panelists pointed at efforts by the United States and the EU in strengthening digital sovereignty and competitiveness, referencing the U.S. CHIPS Act and the CHIPS Act of the EU. The panelists were rather pessimistic regarding the future of China and argued that hopes of a democratization should be abandoned. Instead, the

United States and the EU, as well as other countries of the West, should focus on sustaining a competitive advantage. This required international cooperation and a synchronization of efforts.

Michael Rogers spoke about the "zig-zag" nature of the future, including but not limited to the economic powers of mid-range countries and the changing domain of cyber security. He urged that the best was to brace for the unanticipated and unexpected was to create a rules-based structure.

Conference Day 2, Vantage Point

Mauro Vignati, *Advisor Digital Technologies of Warfare at the International Committee of the Red Cross (Geneva)*

Mauro Vignati laid out how the digitalization of warfare posed new risks to civilians. He highlighted six trends that stood out as particularly worrisome when it came to civilian protection. These were 1) the civilianization of military cyber and digital activities; 2) operations and attacks using dual-use technologies; 3) the changing geography of conflicts through digital technologies; 4) private companies providing their services to states involved in wars becoming parties to the conflict themselves; 5) the provision of digital offensive capabilities from states involved in conflicts to the civilian population; and 6) the varying quality of digital tools deployed in conflict and lack of thorough testing and analysis that could result in collateral damage for the civilian population. He pointed out that in armed conflicts, digital technologies had great potential to support civilians and reduce human suffering. At the same time, he urged: "The task is to ensure that digital technologies were a force for good, instead of drawing civilians closer to the risks of warfare."

Guest of Honor

Kaja Kallas, *Prime Minister of Estonia (Tallinn)*

Moderator: **Stormy-Annika Mildner**, *Executive Director Aspen Institute Germany (Berlin)*

In a Fireside Chat, Prime Minister Kaja Kallas addressed geopolitical developments and their impact on the cyber domain. She also shared insights into Estonia's approach to cyber security and defense.

Asked about the changes she had perceived since the beginning of the war, as well as the learnings, Kaja Kallas pointed out that cyberattacks were not a new phenomenon but that they had increased in number and intensity over the last years, requiring better preparation and foresight. Therefore, partners should share information and analyses of prior attacks. She also argued for a whole-of-society approach, saying that siloed approaches were bound to fail.

Kaja Kallas illustrated how the transformation of Estonian cyber defenses following Russia's large-scale attacks in 2007 could serve as a model for adapting to hybrid threats. She explained

how Estonia deployed cyber audits to identify the weakest links in its digital infrastructure and campaigned to improve media and cyber literacy to increase societal resilience vis-à-vis attacks. Furthermore, she urged victims of cyber-attacks to report incidents, so that all stakeholders could learn and improve. Additionally, Estonia closely assisted SMEs in training and maintaining their cyber hygiene.

Kaja Kallas also underlined the need for international cooperation, for example regarding strategic foresight. "Cyber security is for everybody; cyber security depends on everybody," she stated. Thus, many countries engaged in mapping the cyber dependence of actors and service providers. Based on this ranking of dependency, governments could assess their own strengths and vulnerabilities and use this to inform their defense strategy. Regarding international cooperation, she also touched upon the Global South. Katja Kallas emphasized the need to foster investments in the global South, since China had already invested heavily in digital infrastructure in many countries. In the eye of the global systemic conflict between autocracies and democracies, it was essential that Western countries deepened their cooperation with partners which shared their values, building trusted connections. In doing so, Western countries might prevent China from establishing a power base over these countries and preempt new vulnerabilities when cooperating with them in the future.

Conference Day 2, Closing Keynote

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

Moderator: **John P. Carlin**, *Partner at Paul Weiss (Washington D.C.)*

In the closing keynote of the conference, Lisa Monaco described the strategies of the U.S. Department of Justice in light of increasing cybercrime. In doing so, she assessed the power of the rules-based order and legal frameworks amidst a changing geopolitical environment.

One of the goals of the DOJ was to ensure that law enforcement authorities were used effectively to bring perpetrators to justice while also protecting the privacy of Americans. In pursuing that goal, the DOJ helped shape cyber security legislation and engaged in extensive outreach to the private sector to promote lawful cybersecurity practices.

The U.S. Deputy Attorney General called for an all-tools-approach and urged that there was no time to wait to take action. Strategies should put victims at the center, requiring information and analysis. In a complicated regulatory environment, a critical question was how to balance this with existing regulations such as data protection guidelines. She highlighted that new mechanisms with clear legal frameworks and safeguards were necessary.

The talk then pivoted to the necessity of international cooperation among ministries of justice to counter cybercrime. In this context, Lisa Monaco viewed transatlantic cooperation as vitally important, as every cyber disruption as well as every counter-action had an international dimension. She underscored that none of this work could be done in silos.

Addressing specifically the private sector, she delivered the take-home message that "we are all in this together, and the sooner we recognize this, the better off we will be."

Conference Day 2, Sixth Panel

The Way Forward: Making Alliances Work

Moderator: **Jeff Greene**, *Senior Director for Cybersecurity Programs at the Aspen Institute (Washington D.C.)*

Ciaran Martin, *Professor at the University of Oxford and Former Director of the UK's National Cyber Security Centre (Oxford)*

Vivian Schiller, *Executive Director at the Aspen Institute (Washington D.C.)*

Claudia Gherman, *Senior Policy Manager for Digital Resilience at Digital Europe (Brussels)*

The final panel of the MCSC 2023 addressed the role of alliances in cyber security. Against this backdrop, the panel explored the potential for academia and think tanks to help governments in bridging the public-private divide. A key point was the formalization and institutionalization of advice and partnerships. A trustful, substantive, and productive collaboration could only be achieved in the right environment. It was seen as essential to find ways to leverage the collective wisdom, but also make these processes transparent. Ciaran Martin summarized four takeaways:1) take concrete action, 2) bring along a degree of bureaucratic capability, 3) foster a willingness to take risks, and 4) engage people in the processes.

Vivian Schiller outlined the need for multi-stakeholder cooperation focused on transnational issues. Ideally, stakeholders would pool their knowledge and experience in international, multilateral fora or taskforces that included both public and private voices. Their work should go beyond declarations and truism to make operational contributions and achieve actionable outcomes. In this vein, she noted that the Aspen Institute had established an international, multilateral, private-public cybersecurity forum whose members were global experts collaborating to turn urgent cybersecurity issues into action.

Focusing on the private sector, Claudia Gherman highlighted the potential of advisory councils constituted by senior executives from the private sector to produce actionable recommendations to governments. She highlighted the four areas of governance, procurement, standards, and skills.

All panelists agreed that Russia's war against Ukraine and the subsequent responses of governments as well as private actors was, in fact, a positive example for how a broad alliance of stakeholders could manage to bolster capabilities and share information rapidly. This had a significant impact in elevating Ukraine's cyber defense and fostered its resilience.

The panelists also discussed the transatlantic partnership. While Russia's war against Ukraine had led to increased alignment in the security realm, economic rifts continued to hurt the relationship. As a central hurdle, the panelists identified differences in regulatory philosophies and regulations

on the two sides of the Atlantic. A substantive U.S.-EU partnership on digital information systems, meanwhile, was viewed as rather unlikely. While the EU was indeed seen as a leader in the field, there was little confidence that the United States would follow suit with impactful regulatory action in the next years. Thus, a convergence of approaches and synchronization of efforts were viewed rather unlikely. “Wherever the U.S. cannot or will not act in terms of the information ecosystem, the EU will take the baton,” Vivian Schiller concluded.