Panel I. General cyber security landscape: Strong points and challenges

Moderator: Peter Bátor, Permanent Representative of the Slovak Republic to NATO

- **Kateřina Kalužová**, Deputy Director, Digital Economy Manager, Confederation of Industry of the Czech Republic
- **Andrew Lee**, Vice President for Government Affairs, ESET
- **Csaba Krasznay**, Head of the Institute of Cybersecurity, National University of Public Service
- **Ben Crampton**, Director, European Government Affairs, Microsoft

The panel discussion began with a reflection on the crises that have recently tested our preparedness for various cyber issues and threats. While remote workers lacked security and risk management policy during the COVID-19 pandemic, paradoxically, the overall level of preparedness for cyber threats has increased. This reality is ever so visible today as the unprovoked Russian aggression against Ukraine continues. These attacks have targeted critical and civilian infrastructure, governmental institutions as well as military targets. The goal of these attacks is often to disrupt operations and create chaos. That said, many potentially harmful attacks shave been prevented because Ukraine, having been experiencing similar problems for more than a decade, has learned to build resilience programmes in a way that allows relevant Ukrainian institutions and agencies to detect, deter and respond to malicious cyber activities. Russia's approach to the West, however, has been largely one pursued via diplomatic means while Russia carefully evaluates every move (including in the cyber domain) of the EU and NATO Member States.

The panel discussion continued with the topic of China. The speakers agreed that without a doubt, China has made significant strides in advancing its technology sector in recent years, investing heavily in emerging technologies such as artificial intelligence, 5G networks, and quantum computing. However, Russia and China are not the only players we see on this ‘cyber field’, with North Korea and Iran being particularly active. Their interest in the acquisition of crypto-assets and pursuit of espionage activities was also mentioned. Interestingly, the speakers raised a question as to whether Russia- and China-affiliated groups have been genuinely less actively targeting European entities or whether their ability to do so has improved to the extent that they are being less detected. That said, China’s pivot to the West has not gone unnoticed. All the speakers stressed the need for effective public-private cooperation, without which they will not be able to monitor and understand the evolving cyber threat landscape.

The EU's cooperation with the US was demonstrated by the impact of GDPR, which has also led to increased awareness and concern about data privacy and protection in the US. Many US states have introduced their own data protection laws in response to GDPR. However, panellists expressed their wish to see a more active discussion between NATO and the EU on these topics that are naturally of common interest.

Participants expressed concerns regarding the increasing number and intensity of cyber-attacks on non-governmental organisations and think tanks. This was explained by close links to the government and easy access to information, which the attackers often wish to capitalise on. Questions from the audience also concerned the western technological edge (and whether the West is capable of keeping it) and European investments in innovation in an attempt to bypass the US-China tensions.

Panel II: Cyber and Digital Diplomacy: European values and standards at the edge of digital transformation

Moderator: Liga Raita Rozentale, Independent Strategic Consultant

- **Szilvia Tóth,** Cyber Security Officer, Organization for Security and Co-operation in Europe (OSCE)
- **Marcel Peško,** Ambassador-at-large, Hybrid Threats and Enhancing Resilience Unit, Transatlantic Relations and Security Policy Department, Ministry of Foreign and European Affairs of the Slovak Republic
- **Richard Kadlčák,** Director of Cyber Security Department, Special Envoy for Cyber Space, Ministry of Foreign Affairs of the Czech Republic
- **Engelbert Theuermann,** Ambassador, Special Envoy for Cyber Diplomacy, Federal Ministry for European and International Affairs of Austria

The second panel discussion addressed a set topics covering both external and internal EU tools, existing and yet to be finalised initiatives, and opportunities and threats ahead in the area of cyber. The discussion initially focused on the developments on the UN level, where the EU has ambitions to assert its normative framework amid a visible polarisation on contentions issues. The internal dimension dealt especially with the EU Cyber Diplomacy Toolbox and ways in which the Member States' cooperation could be made more efficient in order to attain joint positions and actions faster, when needed. Importantly, the panel discussion underlined that cyber security and cyber diplomacy go hand in hand.

The panellists agreed that the UN is currently lacking a mechanism that would oversee the implementation of the voluntary norms of responsible state behaviour in cyberspace and pointed toward the proposed Program of Action for advancing responsible state behaviour in cyberspace as a natural successor of the current OEWG, whose mandate ends in 2025. Discussing the EU's involvement in UN policy-making, the panellists agreed that the EU and the like-minded countries' efforts have been insufficient, being merely reactive, lacking a complex strategy and a clear idea of direction. In order to convince non-aligned and undecided UN member states to get behind the EU's vision of cyberspace, including norms and applicability of international law, there is an urgent need to proactively present these countries with tangible arguments. The OSCE could play an important role in this regard and thus should be used (not only) for this purpose. Furthermore, the overarching strategy to pursue these objectives should entail an active involvement of relevant stakeholders, especially private sector entities, whose contribution is already invaluable.

The perspective on the decision-making is seen as a two-step process, with the cyber diplomacy agenda dominating the national level processes while only a part of these information and processes are being transferred and fully made use of on the EU level. It was emphasised that cooperation is often hampered by a lack of trust and strategy. To ensure that the potential of all the platforms dedicated to cyber security and cyber diplomacy does not remain untapped, there is a discussion to be had on how to unify existing concepts, such as capacity building. Additionally, the competences between states, the EU and other institutions should be clearly defined to prevent unnecessary overlaps. In order to create a long-term strategy, more actors ought to be involved as well and trust building at the interpersonal level should be further promoted.

Questions from the audience were focused on the risks of new technologies developed by states with a different system of governance and on the ways in which the EU could strengthen its 'actorness' at multilateral fora.

Panel III: New Techs and Industries: How to embrace emerging technological trends and prepare us for the future? Researchers' perspectives.

Moderator: Marek Čanecký, First Secretary, Information Society, Digital Agenda, Digital Single Market, Permanent Representation of the Slovak Republic to the EU

- **Magdalena Stobińska,** Professor, University of Warsaw
- **Ivan Kotuliak,** Professor, Dean of the Faculty of Informatics and Information Technologies, Slovak Technical University in Bratislava
- **Jakub Harašta,** Assistant Professor, Institute of Law and Technology, Masaryk University
- **Imre Lendák,** Associate Professor, Data Science and Engineering Department, Faculty of Informatics, Eötvös Loránd University

The panel participants looked into the dynamics of the development of digital technologies. They identified Artificial Intelligence and Quantum Technologies as the two most important technology trends that will change the cybersecurity landscape in the future. They are going to bring both – new opportunities and new threats.

When it comes to Quantum Technologies, Quantum Key Distribution is a tool that will radically increase the security of encryption by using quantum effects. While quantum cryptography is already quite mature and might be used in practice in the near future, it is going to take a while till quantum computers will have the computational capacity that will be able to break the currently used encryption algorithms.

A whole new domain is the domain of quantum sensing. It will greatly improve the accuracy of how we measure, navigate, explore and see the world around us by sensing changes in motion, in electric and magnetic fields. This is not only going to bring many new opportunities but it will also bring many security implications.

Artificial Intelligence is not different – one the one hand it will e.g. help us better handle and manage cyber incidents but on the other hand it will enable more efficient personalised attacks as well as creation of immense amounts of fake content at almost no cost.

The speakers also discussed the risk and challenges of these technological developments in terms of human rights and analysed whether currently used legislative concepts are going to be future proof. They agreed that it is going to be more and more difficult to legislate in the fast-evolving technological landscape. One of the solutions might be more frequent use of guidelines instead of legislative acts which are often not flexible enough. As for the rise of quantum cryptography, we will probably see a strong push from the law enforcement sector against stronger quantum encryption. Another big challenge is going to be the review of the personal data protection framework and the fact that it will be very difficult to avoid path dependencies.

Last but not least, the four academics provided information about how cybersecurity and the new technology trends are incorporated in the study programs in their respective universities. Unfortunately, the number of students in these fields does not have increasing trend and is clearly insufficient in the context of the rising demand.

Panel IV: Current Cyber Security Dossiers: Is our framework fit for incidents and threats?

Moderator: Maria Boka, Senior Director at EU Strategy

- **René Baran,** Head of Unit, International Relations and Security Policies Department, National Security Authority
- **Marcin Domagała,** Head of Unit, International Cooperation Division in the Cyber Security Area, Cyber Security Department, Ministry of Digital Affairs of Poland
- **Ádám Vajkovszky,** International policy coordinator, Special Service for National Security, National Cyber Security Center of Hungary
- **Martin Švéda,** Head of the Private Sector Regulation Unit, National Cyber and Information Security Agency of the Czech Republic

The speakers have unanimously shared the opinion that NIS1 has been the first horizontal legal instrument to improve cyber resilience in the EU. It has introduced concrete measures building cybersecurity capabilities and mitigating growing threats to network and information systems. They have stressed two key fundamental changes: (1) The set-up of cybersecurity strategies and legal frameworks which have been mandated by the NIS1 and (2) the directive has for the first time kicked-off a collaboration at Union level, between the respective national cybersecurity authorities, via the NIS Cooperation Group and the CSIRTs network.

However, despite these undisputable successes, the Commission's review of the directive revealed shortcomings. These have been mainly due to the considerable differences in its implementation in member states, such as identification of different entities as essential operators, varying requirements, or supervision methods applied to entities, different thresholds for incident reporting, etc. That caused problems not only for companies operating in several member states, but also undermined the "Union effect", as inadequate implementation in one member state could affect the level of cybersecurity of the others. In the ensuing debate, the four speakers have focused on the state of play of national transposition of the recently adopted NIS2, which is a revision of the previous NIS1 iteration. The key challenge, jointly stressed by all participants, will be to monitor the great amount of entities, now in the scope of the NIS2.

All of the speakers have welcomed the draft Cyber Resilience Act as product-level requirements have been the missing element in increasing the overall resilience in the EU. The panelists have underscored the need to align the incident reporting better between the different legal tools (NIS2, CRA, GDPR) as well as with sector-specific legislation (DORA). For that, member states should be given enough flexibility to devise systems for coordinated incident reporting such as one-stop-shop, as prescribing reporting too narrowly via the different EU lex-specialis, might prevent just that.

When it comes to the recently adopted Cyber Solidarity Act, member states are at early stages of analysing of the proposal. However, from the first indices, the question arises whether transferring of funding which was previously allocated for implementation of the default legislation, into the newly proposed structures, as well as "by-passing" of the newly created European Cybersecurity Competence Centre in Bucharest, is the right way forward.

Finally, the speakers agreed on the need to focus on effective implementation of the default rules on the national level and making sure the different pieces of legislation are well aligned and complied with by the industry, before adopting new proposals.