Programme

Date: 25 May 2023

Venue: Permanent Representation of the Slovak Republic to the EU, Brussels

08.15 Registration and coffee

08.40-08.45 General introduction

08.45-08.50 Welcome remarks

- **Petra Vargová**, Permanent Representative of the Slovak Republic to the EU

08.50-09.00 Keynote speech

- **Rastislav Janota**, Director, Slovak National Cyber Security Center

09.00-10.30 General Cyber Security Landscape: Strong points and challenges

The panel will elaborate on the current general security threats and challenges with a specific focus on cyber security predominantly in the region of Europe, the United States and Asia. In the pressure of the events in Ukraine following February 24th 2022, which broke the post-WWII silence, Europe, America and dozens of countries worldwide launched multiple actions. The EU, long criticized for a limited ability to decide and act, got fast united and ignited a series of unprecedented responses.

On the other bank, Russia stimulated by the muted giants of Asia has turned into a savage barbarian plundering its fellow neighbour, but with no major success. The hits of crises of COVID-19, the demand-supply chain, energy and inflation underpinned by the ecology and migration megatrends have brought civilisation to a new crossroads at the very edge of history. Modern warfare enables novel weapons, systems and methods, where sophisticated cyber campaigns play a crucial role. The panellists are expected to give their views on the ongoing situation. The audience might hear how far the malicious cyber interference has developed, whether the large-scale attacks have worked, whether cyber activity by actors stemming from Russian territory and other countries has increased and what consequences have it induced. Our guests will be invited to give their outlooks on future development. How the world will be changed or not?

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

10.30-10.45 Coffee break

10.45-12.15 Cyber and Digital Diplomacy: European values and standards at the edge of digital transformation

In recent years, foreign policy's cyber and digital aspects gained considerable traction. Already in 2016, NATO Allies recognized cyberspace as a domain of operations and a possible armed conflict. Since then, the EU has adopted multiple initiatives to bolster the EU and Member States' diplomatic response to malicious state and non-state behaviour in cyberspace. The Cyber Diplomacy Toolbox, for instance, allows for a coordinated diplomatic response to such acts and is part of the EU's wider approach to Cyber Diplomacy within the Common Foreign and Security Policy. On the digital side, the ITU has become an area of strategic competition and geopolitical controversies as even tech standards have been permeated with political interests. Similarly, the Internet has faced attempts to challenge its global, open and transparent nature.

This is mainly relevant in the UN context where the Global Digital Compact is expected to 'outline shared principles for an open, free and secure digital future for all' but also in connection to the OSCE, OECD and the Council of Europe, where the Convention on Artificial Intelligence is currently being negotiated. These developments pose questions about how international relations affect standard-setting processes and the extent to which the EU and its Member States are able to stand their ground and keep their interests and values at the forefront. The second panel will be devoted to Cyber and Digital Diplomacy and the discussion will focus on how to ensure closer and more effective cooperation between the EU and its Member States in the cyber and digital fields, aiming at a more assertive and influential position of the EU on the global stage.

Moderator: **Līga Raita Rozentāle**, 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
- **Bert Theuermann**, Ambassador, Special Envoy for Cyber Diplomacy, Federal Ministry for European and International Affairs of Austria

12.15-13.30 Buffet lunch

13.30-15.00 New Techs and Industries: How to embrace emerging technological trends and prepare us for future? Researchers' perspectives

The current period of technological evolution is proving to be the most disruptive one in history, surpassing even the advent of the internet. Emerging technologies and ongoing research and innovations in domains such as artificial intelligence and quantum computing are set to bring about wide-ranging implications for our society and economies, including new cybersecurity risks and threats. Implementation of some of these technologies in real-life use cases has already begun to change the way people live, learn, work, and socialize. For example, AI helps companies to interact with their customers more effectively. AI helps doctors to better treat their patients. AI helps governments to provide their services more efficiently. At the same time, to name just a few risks: There is growing evidence of AI being used by hackers and malicious actors. AI also makes the generation of disinformation and deep fakes far easier than in the past. Quantum technologies might not be as mature as AI at this moment, but the benefits and the risks they will bring in the future are equally considerable.

The EU must be ready to embrace the benefits stemming from technological trends, but while doing so we must not lose sight of the EU's core values and human rights. A better understanding of the dynamics of how emerging technologies are changing and will change our understanding of cybersecurity will help us do so more effectively. Based on the latest scientific evidence, the panel aims to examine the impact of the above-mentioned emerging technologies on cybersecurity and highlight the key ethical and human rights implications and risks they pose.

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**, 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 (DSED), Faculty of Informatics, Eötvös Loránd University

15.00-15.15 Coffee break

15.15-16.45 Current Cyber Security Dossiers: Is our framework fit for incidents and threats?

The main debate of our panellists should point out where we actually stand with cyber and respective digital legislation with cyber elements and whether the current legislative framework is fit enough to catch up with the latest threats and cyber trends. The previous year of 2022 was quite rich in various cyber dossiers, such as the updated Network and Information Security Directive (NIS), Cyber Security Act (CSA) implementation via the ENISA's work on cyber certification schemes and Bucharest-based European Cyber Competence Centre (ECCC) and, last but not least, the Cyber Resilience Act (CRA) proposal. Just apart from those there are several other files, mostly in sectoral fields, consisting of or relating to cyber components. The panellists will be asked whether Europe is ready and able to secure European citizens and industries. Is the current organisational chart of European institutions, bodies and agencies fuel-charged with the right competencies and working effectively or is there quite an intricate picture of numerous entities unable to act swiftly, efficiently and in a transparent manner? What is missing in the European setup?

Moderator: **Maria Boka**, Senior Director, 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, Single point of contact, 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

16.45 End of conference