FORUM CYBERSECURITY

Ministry of Digital Affairs
Republic of Poland

NASK

Enhancing Cooperation
How to Better Manage Cyber Crises?

Cyber Ministers' Meeting (EU27 + candidate states)
4th September 2024, Karpacz, Poland
High-Level Exchange of Views

Amid growing cyber threats new legislation and initiatives, discussing how to best coordinate our cyber efforts is crucial. Building the bridges and connecting the dots in cybersecurity require team effort. The current geopolitical situation and the fast pace of technological development demonstrate the need for enhanced civil-military cooperation and synergies. Securing our critical infrastructures is vital, yet the level of cyber maturity varies across sectors. Healthcare systems as well as other critical sectors are increasingly the target of cyber and ransomware attacks. Despite the ongoing efforts to address the cybersecurity skills gap, its persistence poses challenges to Europe's cyber capabilities. Sustainable and future-oriented cybersecurity financing ideas might be useful for moving forward.
Navigating towards a strong and secure Europe calls for a holistic approach and collaboration among like-minded countries. There are at least several areas deserving closer examination by our community, including the civil-military cyber cooperation, state and non-state actors, global IT disruptions, cybersecurity of healthcare as well as cyber skills gap. We see much value in preliminary exchanges on these issues under the following guiding questions.

QUESTION 1 CIVIL–MILITARY CYBER COOPERATION:
The development of coherent, complementary and interoperable defence capabilities, avoiding unnecessary duplication, is key in our joint efforts to make the Euro-Atlantic area safer. What can be done to enhance the civil–military cyber cooperation and ensure better alignment of actions? What are the biggest challenges and how can we address them? What are the lessons learned from successful collaborations, projects, structures etc. involving civil-cyber and military-cyber personnel? Do you see added value in building such competences together?

QUESTION 2 STATE AND NON-STATE ACTORS:
We encounter challenges, among others, from state and non-state actors as well as criminal entities, often cooperating maliciously with each other. What could we do more together to combat threats coming from various types of actors?

QUESTION 3 GLOBAL IT DISRUPTIONS:
The recent global IT disruptions caused by a faulty CrowdStrike software update could be considered a stress-test for cooperation at various levels. What is your initial assessment of the collaborative aspects of handling the incident, including at the international level? How can we strengthen the existing cooperation?

QUESTION 4 CYBERSECURITY OF HEALTHCARE:
A European action plan for cybersecurity of hospitals and healthcare providers is to be proposed as mentioned in the Political Guidelines for the next European Commission 2024-2029. What are the key challenges associated with cybersecurity of health systems and how to address them? How do you asses the cyber threat awareness level in that sector?

QUESTION 5 CYBER SKILLS GAP:
According to a foresight report by ENISA, the cyber skills gap is a significant factor contributing to increasing cyber threats. How do you tackle this challenge? What else can be done in your opinion to facilitate the access to cybersecurity professional trainings? What are your recommendations on how to:

- *address talent shortages in cyber security;*
- *tackle cyber security skill shortages with the involvement of industry and governments;*
- *make cyber security education and training more inclusive and flexible?*