Conference on Cyber Issues
under the Slovak Presidency in the Council of the EU

14 December 2016

- Brief summary -

More than 180 decision makers and stakeholders discussed the current cyber issues topics in five domains (cyber security, cyber research and development, cyber crime, cyber defence, cyber diplomacy). The main outcomes are summarized below:

Panel on Cyber Security

- ✓ Two recent European important initiatives are mobilising public and private stakeholders for improving cybersecurity:
  a) the Public-private partnership on cyber security was launched in July that will trigger €1.8 billion of investment by 2020.
  b) the Network and Information Security (NIS) Directive, which was adopted in July 2016 and involves setting up a network of computer security response teams across the EU in order to rapidly deal with cyber threats and incidents.

- ✓ The NIS Directive will improve national cyber security capabilities across the EU, which is unevenly developed. Member States that need to improve their capacity to respond to digital threats need to catch up with those that are already better prepared.

- ✓ There will also be security and reporting obligations for companies managing critical infrastructure in key economic sectors such as energy, transport and banking, which use digital networks to provide their services. Similar obligations will apply to key digital service providers. Each EU Member State and company covered by the new rules will need to take on their share of responsibility to manage shared digital risks (new incentives may be considered in this respect – such as cyber insurances).

- ✓ As our economies become ever more interconnected and digitalized, they also become increasingly vulnerable and exposed to cyber threats. Therefore continuous work will be needed to address the ever-growing number and complexity of cyber threats.

- ✓ Working together in Europe on improving cyber security clearly makes more sense than working in isolation. This will also help build the essential level of trust and confidence in the European digital economy and society.

Panel on Cyber Crime

- ✓ The issue of e-evidence is more far reaching than the scope of cybercrime as electronic evidence is also relevant in cases of traditional/conventional crime.

- ✓ The need to keep initiatives coherent and not to duplicate the work is necessary.
- ✓ The issue of encryption is sensitive but important one. Stakeholders appreciate that the current policy approach aims at supporting benefits that the encryption can bring to individuals and businesses.

Panel on Cyber Research and Development

- ✓ The research agenda has to set clear priorities which will prevent the investment from diluting into too many different realms.
- ✓ The cPPP on cybersecurity has to build on available technologies and develop them further to provide adequate response to the evolving cybersecurity threat landscape and enhance European autonomy and competitveness.
- ✓ Research in cyber security has to focus not only on technological aspects but also on societal aspects, essential part of the R&D agenda is trust building and education.
- ✓ Cyber security has to be mainstreamed into core activities of businesses and industrial sectors and key industrial sectors.
- ✓ One of the greatest challenges in cyber security R&D is the IoT phenomenon due to the vast and growing number of IoT devices.
- ✓ It is important for users and operators to participate in the cPPP in order to better follow market needs

Panel on Cyber Defense

- ✓ The recognition of cyberspace as an operational domain will help NATO to have a more dynamic position, taking into account that every future conflict will have a cyber component.
- ✓ Cyber defence should be considered as early as possible in the planning and conduct of EU-led military Operations and Missions.
- ✓ Cybersecurity should be ensured as much as possible "by design".
- ✓ Cooperative initiatives such as the cyber hygiene initiative has great potential to increase end-user awareness.
- ✓ The growing number of applications and programs running on systems conducts to more vulnerabilities.
- ✓ A lot if cybersecurity solutions are dual-use, and can be used in both military and civilian context.

Panel on Cyber Diplomacy

- ✓ The importance of cyber diplomacy for the future European security policies is growing given its role and ability to coordinate and govern international relations in the field of cyber. It is clearly recognized that this process should primarily lead to global cyber stability and international security. The semantics and role of cyber diplomacy is one of the top candidates to be incorporated in the next EU Cyber Security Strategy revision.

- ✓ Several key components are necessary to build effective and resilient global cyber security system, notably: a) norms of behaviour and application of existing international law; b) cyber capacity building; c) internet governance; d) strategic engagement in international organisations.

- ✓ Policy makers and relevant stakeholders should maintain the open and transparent discussions with a high working momentum and continuous efforts.

- ✓ As a positive example of international cooperation under the United Nations umbrella, activities of the group of governmental experts on cyber security (UNGGE) were mentioned, especially in relation to the ongoing discussion on cyber norms.

- ✓ Panelists futher acknowledged the outcomes of the WSIS+10 process which was successfully finalized in December 2015, welcomed the historic IANA functions stewardship transition to multistakeholder community from October 2016 and stressed the added value of the ongoing international cyber dialogues with global partners, notably between the US and EU.