Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025
28 March – 1 April 2022

Key EU messages for Agenda item 5: on Threats and Initiatives of States aimed at ensuring security in the use of ICTs

Mr. Chairman,

I have the honour to speak on behalf of the EU and its Member States.

The Candidate Countries North Macedonia, Montenegro, and Albania, the country of the Stabilisation and Association Process and potential candidate Bosnia and Herzegovina as well as Ukraine, the Republic of Moldova, Georgia and San Marino, align themselves with this statement.

1. Cybersecurity is an integral part of one’s security. Whether it is connected devices, electricity grids, banks, aircraft, public administrations or hospitals, people deserve to use and trust these services with the assurance that they will be protected from cyber threats.

2. Our economy, democracy and society depend more than ever on secure, reliable and increasingly interconnected networks and information systems. Cybersecurity is therefore essential for building a global, open, free, stable and secure cyberspace.

3. Cyber-attacks targeting our critical infrastructure, democratic institutions and processes, public core, supply chains and intellectual property are ever increasing. These activities undermine international security and stability and the benefits that cyberspace brings for economic, social and political development.

4. In 2020, 742 cybersecurity incidents with significant impact against critical sectors were reported in the EU. In 2019, this number was 432. This represents an increase of 72%. And cyberattacks have continued to increase through the years 2020 and 2021.

5. Concerns about security are a major disincentive to using online services. One in eight EU businesses have been affected once by cyberattacks. Improving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights
to privacy and to the protection of personal data, and the freedom of expression and information.

6. As technology becomes inextricable from the physical world, cyberattacks can put the lives and the wellbeing of the most vulnerable at risk, as well as risk misunderstanding and escalation in cyberspace.

7. We are very much concerned of the recent waves of cyber-attacks which have a global range and consequences as Solar Winds and Microsoft Exchange. We have seen the impact and spill-over effects such cyber-attacks can have with the cyber-attack NotPetya in 2017 conducted by the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU). And the number of cyber-attacks targeting our governments, our critical infrastructure, our intellectual property, supply chains and democratic processes is ever increasing.

8. Threat actors associated with the Russian state have last year alone targeted numerous members of Parliaments, government officials, politicians, and members of the press and civil society in the EU by accessing computer systems and personal accounts and stealing data. Such activities are unacceptable and contrary to the norms of responsible State behaviour in cyberspace as endorsed by all UN Member States, as attempt to undermine our democratic institutions and processes, including by enabling disinformation and information manipulation.

9. Also Russia’s unprovoked aggression against Ukraine, including in cyberspace, is of greatest concern and in violation of international law and breaching the norms of responsible state behaviour that we have all agreed upon here in the United Nations. We have sadly seen the use of cyber-attacks involving destructive instruments such as wipers for system breakdown, but also service disruptions, intrusion attempts, defacements and DDoS attacks targeting Ukraine, with the potential for spillover into other countries, particularly Ukraine’s neighbours.

10. We in addition see a rising number of uncoordinated actions by volunteer hackers and hacker groups. These activities cause – again - an increased risk of spillover of cyber incidents and affecting other countries if they get out of control. Cyber-attacks may also
trigger chain reactions throughout the economy and society, affecting millions of individuals, as well as international security and stability.

11. In the EU, illegal access to information systems, illegal system interference and illegal data interference where intentional, is punishable as a criminal offence (Directive on attacks against information systems 2013/40).

12. Preventing and limiting malicious activities is of crucial importance, reducing the risk of miscalculation and escalation, and we should all respect international law and norms of responsible state behaviour.

13. The respect for international law, including international humanitarian law and international human rights as well as the norms of responsible state behaviour, is crucial to achieve international security and stability in cyberspace.

14. This makes the implementation of the UN framework for responsible state behaviour particularly pertinent in view of international security and stability, notably through the OEWG as well as the Programme of Action to Advance Responsible State Behaviour in Cyberspace.

15. Through the respective EU Cybersecurity Strategies, the EU and its Member States have invested significantly in legislation, policies, measures aimed at appropriately addressing cyber threats and activities.

16. Computer Emergency Response Teams have been established, in cooperation with the private sector and crisis management structures have been set up, all in effort to address the increasing number of cyber threats. All these activities are directly contributing to the implementation of the UN framework. Later this week we will elaborate on our activities that support third countries in building similar preparedness against cyber threats.

17. In addition, the EU has put in place external policies and mechanisms to address growing challenges, notably to advance the UN framework for responsible state behaviour in cyberspace, and to design and implement diplomatic responses to malicious behaviour in cyberspace that is in contradiction with the UN framework, with the aim of conflict prevention and stability in cyberspace.
18. The EU and its Member States believe we should continue to elaborate and exchange on the cyber threat landscape, the consequences for international stability and security as well as our societies and economies, and the ways and means that could support States to tackle effectively the most pertinent security challenges in cyberspace.

19. In order to develop a common understanding to tackle the pressing challenges faced by all States, the OEWG could hold dedicated meeting on specific norms of responsible state behaviour in light of specific cyber threats faced by the broader international community.

20. Such discussions would contribute to the understanding of the cyber threat landscape, the challenges to be addressed by the international community, as well as the need to advance the implementation of the UN framework for responsible state behaviour.