Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025
11 – 15 December 2023

Key EU messages for Agenda item:
Existing and Potential Threats

Excellencies,

I have the honour to speak on behalf of the European Union and its 27 Member States.

The candidate countries North Macedonia*, Montenegro*, Albania*, Serbia, Ukraine, the Republic of Moldova and Bosnia and Herzegovina*, the potential candidate country Georgia, and the EFTA countries Iceland and Norway, members of the European Economic Area, as well as San Marino align themselves with this statement.

The European Union and its Member States strongly condemn malicious cyber activities targeting democratic institutions and electoral processes. We closely monitor any attempts of cyber-attacks on our democratic processes, especially in the context of the upcoming European elections. As pressure is mounting on democracy globally, we continue assisting and working with partners against these ongoing cyber threats. In this vein, the European Union and its Member States share the serious concern of the United Kingdom and other partners as stated in their declarations on December 7th and express our full solidarity. Activities that seek to threaten our integrity and security, democratic values and principles and the core functioning of democracies are unacceptable.

Those activities are contrary to the norms of responsible state behaviour in cyberspace as endorsed by all UN Members. We continue to promote due

**North Macedonia, Montenegro, Serbia, Albania and Bosnia and Herzegovina continue to be part of the Stabilisation and Association Process.*

diligence and responsible State behaviour in cyberspace and call upon all states to comply with these norms and principles.

Technological and political changes are reshaping cyberspace and the ways that people interact with it. Working together to understand the evolving nature of the threat of malicious cyber activity is crucial to setting the context in which we develop practical measures for international cooperation.

In 2022 the number of software supply chain attacks tripled. Every day, small businesses and critical institutions, including hospitals are being targeted by cyber criminals. Every 11 seconds, an organisation is hit by a ransomware attack, with an estimated cost of €20 billion annually.

The increasing scale and severity of ransomware attacks is one element which heightens the risk to essential services and critical national infrastructure, and may therefore rise to the level of national and international security. In the longer-term, we anticipate witnessing more complex and high profile malicious cyber activities driven by AI-powered software.

There is little doubt, that humankind is on the verge of an era of exponential technological advancement, and AI is leading the way in the emerging digital world. For cybersecurity, this trend has comprehensive implications. In simple terms, artificial intelligence acts as a powerful catalyst and enabler for cybersecurity in our connected ecosystem.

Furthermore, AI-powered cyber defences can detect and respond to cyber threats in real-time, bolstering military network security against attacks. This duality of AI has implications on peace and security, and it underscores why AI is likely to challenge the way we have been dealing with technology and the concept of dual use until now.

**North Macedonia, Montenegro, Serbia, Albania and Bosnia and Herzegovina continue to be part of the Stabilisation and Association Process.*

Russia’s illegal aggression against Ukraine shows that ICTs are an integral part of modern warfare. In this context, malicious cyber activities are capable of causing excessive harm to civilian infrastructure and critical energy infrastructure. As reported by Ukrainian authorities, the overall number of campaigns originating from Russia-aligned threat groups against Ukraine doubled in the last six months.

It is important to note that while the threats that we face are evolving and increasing, we have a framework, which we have all agreed to, as our collective starting point to address these threats. The threats just mentioned, as well as the threats that will be raised by our colleagues here today and in past sessions, provide the context against which the following discussions under our mandate flow, and the context through which the work of this group becomes meaningful.

Just as creating a clear link between the existing and emerging threats we identify, and the remainder of our work discussing recommendations and proposals for responsible use of technology – through the application of international law, norms, CBMs and capacity building.

We look forward to further advancing discussions, including expert briefings with a deep dive into on this important topic inside the OEWG in the years to come.

**North Macedonia, Montenegro, Serbia, Albania and Bosnia and Herzegovina continue to be part of the Stabilisation and Association Process.*