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. Being derived from international law, rules, norms and principles of responsible state behaviour are key to maintaining international peace, security and stability.

2. Enhancing our common understanding about these rules, norms and principles and advancing their implementation should be at the core of our common efforts.

3. The OEWG is not the first attempt by UN Member States to consolidate common rules for cyberspace. Six consecutive UN Groups of Governmental Experts (GGE) met between 1997 and 2021.

4. The most notable development stemming from the UN GGE process was the adoption of consensus reports in 2010, 2013, 2015 and 2021 outlining and reaffirming a set of foundational norms of responsible state behaviour in cyberspace and reaffirming that international law, including international humanitarian law and human rights law, apply to cyberspace.

5. These developments serve as the basis for our subsequent discussions, including those at the OEWG today.
6. In this regard, the first OEWG has elaborated on and strengthened the 11 norms of responsible state behaviour, in particular by enhancing the understanding of the implications of these norms of responsible state behaviour.

7. Our continuous exchanges should now further clarify our expectations on these norms, and should present best practices on putting them in use.

8. In this light, let me highlight some of these expectations, for instance with regard to norm 13(f) from the UNGGE 2015 report, reading “A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public”.

9. Contrary to the expectations set, Russia, who has been at the core of the development of the UN framework for responsible behaviour in cyberspace, and as a permanent member of the UN Security Council, has attempted to interfere in Ukrainian elections, targeted its power grid, defaced its government websites and spread malware in their systems with destructive effect. Behaviour that is seriously violating the UN framework of responsible state behaviour in cyberspace.

10. Norm 13(c) of the UNGGE 2015 report states, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs". What is expected, is that States act in line with their obligations under international law, and perform due diligence, including by preventing their territory to be used by cyber criminals as well as prosecuting them. States are in this regard expected to build a solid cyber security framework, with a cybersecurity strategy and cybersecurity legislation at its core, that provide measures to boost the overall level of cybersecurity and prevent cyber-attacks from taking place.

11. The EU has stepped up its efforts to ensure to adhere to the UN framework, including through the Directive on security of network and information systems as well as increasing inter-institutional and intra-EU cooperation to enhance coordination of cybersecurity crisis management. Most recently, we have issued a set of cybersecurity best practices, and encouraged all public and private sector organisations in the EU to apply these practices to improve their cyber resilience.
12. To achieve results and address the urgent need for security and stability in cyberspace, the EU and its Member States believe that our discussions in the OEWG should urgently invest in exchanging best practices on the implementation of the UN recommendations provided, and to contribute to the national survey of implementation of the UN General Assembly Resolution 70/237 in this regard.

13. We should also invest in enhancing the practical capabilities of all States in the area of implementation of norms. The EU and Member States stand ready to elaborate on the implementation of their EU Cybersecurity Strategy adopted in 2020 to share its experience through capacity building efforts on the implementation of the UN framework for responsible state behaviour in cyberspace, as well as on improving the resilience and incident response capacities.

14. The EU and its Member States look forward to work with States and other stakeholders to take forward these efforts, including through a dialogue on the contribution by a Programme of Action a permanent and inclusive platform in the United Nations to the joint work on the implementation and capacity building.