Mr. Chairman,

Montenegro aligns itself with the statement delivered by the EU.

All over the globe we are in a position to benefit from the rapid exponential growth of information and communication technologies, harvesting important social and economic incentives and opportunities from being connected and be a part of the raising Internet-based economy. However, while our societies more and more rely on digital infrastructure, technology is still vulnerable.

Privacy, integrity, availability of the infrastructure is more and more challenged by rapidly evolving cyber threats due to malicious use of ICTs by all kinds of actors present in cyberspace: they used to be just hackers, but nowadays they are criminals, terrorists, state and non-state actors. Cyber-crimes and threats undermine not just the safety of network users, but disrupt economical and commercial activities all the way to influencing military effectiveness and transferring the real sphere conflicts directly into cyber domain. With new technologies classical warfare has already been taking the forms of the hybrid warfare, destabilizing the international security landscape.

In such circumstances, the multilateral approach represents the optimal response to keep the transformational power of ICTs in its role of social and economic development catalyst, preventing erosion of the citizens’ and national trust and confidence in the use of ICTs.

Montenegro is fully committed to contribute towards creating conditions for a free, stable, transparent and secure cyberspace. Out of our own specific experiences, we are supporting a multi sectorial and multi stakeholder approach in protecting cyber environment as well as organizations', institutions' and citizens' assets. In essence, it has to be a holistic approach, with human security in its center, which will enable effectiveness in tackling risks associated with cyber-crime and more sophisticated cyber-threats, while taking into account the rule of law and good governance. Additionally, it is also important to emphasize that any process that might lead towards modifying the ability of any individual to benefit from ICTs due to national or other security reasons has to be transparent, inclusive and accountable.
We support the coordinated work of the UN Group of Governments Experts and the Open-Ended Working Group, and we will take part in the ongoing discussions on cybersecurity within the work of the UN First Committee.

It is of the great importance to keep the momentum showed during the OEWG first substantive session and we will be further on engaged in accordance with the work schedule presented by its Chair, while working on creating and promoting a comprehensive framework to advance peace and stability. We are confident that in such a manner we will have a better position to reaffirm the central role of United Nations as a global leader in cybersecurity, ensuring trust, confidence and protection of citizens, industry and whole societies.

Thank you.