Mr. Chair,

Hyperactive development of IT-technologies progressively led to the “re-formatting” of internet space: nowadays it is no longer a comfortable platform for communication, but also a real weapon, which becomes more and more dangerous in hands of hackers and criminals.

In fact, cyber-attacks have become a new method of hybrid warfare. Such warfare of a new generation is more convenient and less expensive than a classic war – it is enough to hire a group of hi-end IT specialists who, by using specially created software, can break targeted computer servers and deactivate almost any navigating system of any type of weapon.

As of today, threats to critical infrastructure typically range from malicious actions of a non-state actors, including those sponsored by certain States, to natural disasters.

Non-state actors are specially trained to shut down nuclear power plants, disconnect airport navigation, mislead hi-speed trains, paralyze hospitals and make your routine life unpredictable, chaotic and restless. On the highest level, they can interfere in elections of the parliaments and nominate governments. They impact on global security and political stability in the world.

Some States use high technologies to get their own political and geopolitical objectives, namely by supporting and exacerbating conflicts in other States, conducting aggressive propaganda, campaign and information wars.

Given the current cyberspace landscape, the protection of critical infrastructure remains a top priority subject for most governments and private sector representatives simply because it touches an everyday life of each of us. We consider the issue of protecting of critical infrastructure from malicious ICT activities more political than purely technical one.

In this vein, we emphasize the importance of recognition in the reports of the previous OEWG and the GGE of the fact that certain States use ICT capabilities for military purposes.
We believe that the OEWG should discuss meaningfully cyber threats that affecting international peace and security, including the risks of miscalculation that could lead to escalation of tensions, whenever cyber incidents between States take place.

Ukraine is a strong supporter of the idea that ICT shall be used only as a tool for development, according to the provisions and principles of the UN Charter. Transparent and inclusive international dialogue, based on the principles of openness, could stop and prevent the current active usage of ICT as a method of fueling conflicts and hostility.

In this regard, it is important for States to play in fostering ICT security and improving their own cyber-ability to resist internet-based threats and enhance our common cyber resilience policy taking into account latest challenges and threats in the use of ICT.

Thank you, Mr. Chair