Open Ended Working Group in the Field of Information and Telecommunications in the Context of International Security

Existing and Potential Threats

Statement by H.E. Nathalie Jaarsma
Ambassador at-Large for Security Policy and Cyber

NEW YORK, 15 December 2021
**Existing and Potential Threats**

Thank you, Chair.

In our modern world, cyberspace has become a pillar of our society, bringing economic growth and social progress to our citizens. It increases access to information, knowledge and development, allows for greater and faster innovation, facilitates the free flow of new ideas and opinions and in a growing number of societies it is a means for citizens to efficiently access essential services. These benefits are enhanced by the global, open, free and interoperable nature of the internet, which the international community should uphold and promote.

However, the Netherlands is deeply concerned with the increase of malicious ICT activities in cyberspace and the misuse of ICTs. Such activities have a direct impact on trust and increase the risk of escalation and conflict in cyberspace and beyond.

In our national Cyber Security Assessment, the Netherlands assesses that disruption and sabotage have the most impact on national security because of their potentially disruptive effects on society and wellbeing of our citizens. This also includes theft of Intellectual Property.

From the Netherlands’ perspective, aggressive and coercive ICT operations below the threshold of actual armed conflict, and ICT activities to prepare them, are occurring more regularly and constitute an urgent challenge to international peace and security.

Chair,

Some examples of existing challenges and potential threats that the global community is facing include cyber operations against the integrity, functioning and availability of the internet, as referred to in the acquis. This technical infrastructure essential to the general availability or integrity of the internet, or the **public core**, was referred to on critical infrastructure in both the previous OEWG and GGE reports (*norm 13f*).

This technical infrastructure essential to the general functioning of the internet also needs **protection** against tendencies to control it in a way that would undermine the integrity or availability of the internet. We see these tendencies coming from a broad range of actors.
In particular, the Internet governance model, which is based on multistakeholder governance, should in no way be undermined. The private sector, civil society, technical community and other stakeholders are indispensably connected to the functioning of the Internet.

Recent developments have also reaffirmed that operations against critical infrastructure more broadly are problematic and constitute a threat to international peace and security. In this context, we again highlight threats against for example the healthcare sector and electoral processes.

In addition, new and emerging ICT’s and their use in malicious cyber-operations is an area of increasing concern. The OEWG should therefore not be blind to threats arising from new developments, and should stress that States should at all times respect the UN consensus framework in their use of such technologies.

States experience different impacts by malicious ICT activity. Through its discussions, the OEWG can help ensure capacity building is sensitive to these differences and increase States’ resilience. The National Survey proposed by Australia and Mexico during the previous OEWG could be a helpful tool in this regard as it identifies potential gaps where capacity building can help.

Chair,

The Netherlands attaches great value to the agreed normative framework of responsible State behaviour. The agreed norms, especially via the additional layer of understanding developed in the GGE report, provide useful suggestions to address threats.

We can enhance the application of the framework by concrete implementation, for example by Regular Institutional Dialogues as the Programme of Action.

Moreover, it should be stressed that voluntary, non-binding norms are not non-committal. In addressing existing and potential threats, we are convinced that building the capacities to implement the normative framework will significantly strengthen international peace and security and allow all States to enjoy the benefits of ICTs. It is up to responsible States to uphold the norms and address each other in case of non-compliance.
Chair,

Finally, the OEWG should adopt a human-rights based approach when addressing threats. It has to be crystal clear that cybersecurity and human rights are not competing values or interests, but are interdependent and mutually reinforcing. Threats to cybersecurity are more often than not also threats to human rights, examples may be privacy concerns arising from surveillance practices as well as threats to the availability or integrity of the Internet which have implications for access to the Internet. In a growing number of societies, no access to internet means no access to certain essential services.

Any measures aimed at improving cybersecurity should be in full conformity with human rights law and comply with our international obligations deriving from it.

Thank you.