Opening of the First Substantive Session of the Open-Ended Working Group on security of and in the use of information and communication technologies 2021-2025

Remarks by Ms. Izumi Nakamitsu
High Representative for Disarmament Affairs

Check against delivery

New York
13 December 2021
H.E. Ambassador Burhan Gafoor, Mr. Chair,

Distinguished delegates,

It is an honour to address the opening of the first substantive session of the new Open-Ended Working Group on the security of and in the use of information and communication technologies.

You embark on a 5-year mandate, yet the need to address the peace and security challenges arising from the malicious use of ICTs remains urgent.

Incidents involving the malicious use of ICTs by State and non-State actors continue to grow.

The increasing sophistication and diversity of these incidents harm peace and security, human rights and sustainable development.

Mistrust linked to the digital domain is on the rise.

And an ever-expanding ICT “attack surface” is exposing new vulnerabilities.

While the cyber threat landscape is daunting, there is reason for optimism.

The successful conclusion of two recent intergovernmental processes this year marked a high point in multilateral efforts to ensure a safe, secure and peaceful ICT environment.

I extend my gratitude to Ambassador Patriota and Ambassador Lauber for their tremendous efforts in bringing that work to a successful conclusion, particularly in the face of ongoing challenges posed by the COVID-19 pandemic.

I also applaud the tremendous flexibility and dedication of all delegations, which contributed to substantive and concrete results.

The first Open-Ended Working Group, in particular, represented a significant milestone in preventing and mitigating the impact of malicious ICT activity.
Building on the foundation established by the expert groups, the Working Group painted an increasingly clearer picture of cybersecurity risks, while elaborating recommendations to address them.

Mr. Chair,
Distinguished delegates,

As many delegations have already highlighted, this Working Group is not “starting from scratch”.

The General Assembly has recognized the elaboration of an initial framework, comprised of concrete norms of responsible State behaviour and international law underpinned by capacity-building.

The norms aim to ensure cooperation and information exchange, to prevent escalation including because of misattribution of responsibility, and to uphold human rights.

Protection of critical infrastructure continues to be of particular concern. For example, much attention has rightly been drawn to the potential devastation of a malicious cyber activity directed towards the healthcare sector amidst a public health emergency like the current COVID-19 pandemic. It is notable, in this connection, that three of the eleven norms aim to protect such assets. This includes a requirement to refrain from conducting or knowingly supporting ICT activity that intentionally damages such infrastructure or otherwise impairs its use or operation.

Alongside norms, States have identified common principles and processes related to building the capacity of all States, in order to ensure they have the ability to prepare and respond to malicious ICT activity.

And governmental experts have elaborated additional understanding on the applicability of international law to cyberspace, while committing to study this topic further.
As important as these achievements have been, more can and should be done.

In this regard, I wish to highlight three key areas for dedicated attention where further work is required and where this Working Group could make meaningful contributions to a safe and secure ICT environment.

First, I encourage delegations to identify practical measures to effectively implement the agreed normative framework, at the subregional, regional and global levels.

Such measures can include reviews of national and regional strategy frameworks on the basis of voluntary reporting or peer-to-peer review processes.

Confidence-building measures and international cooperation to build national capacities can also help States develop means to detect, attribute and respond to ICT-related incidents.

Second, States must commit to further unpacking of the applicability of existing international law to cyberspace, including international humanitarian law.

As an essential baseline, States have affirmed that international law, in particular the UN Charter, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. This is a fundamental common understanding.

Nonetheless, it is critical that States discuss concretely how international law applies to cyberspace, including acts carried out in the context of armed conflict that might result in the incidental loss of civilian life, injury to civilians or damage to civilian objects.

In line with the recommendation of the first Open-Ended Working Group, I encourage States to continue to inform the Secretary-General of their assessments of how international law applies to their use of ICTs in the context of international security.

Even where divergences exist, exchange of national views and practices can support greater predictability and reduce miscalculation.
As a contribution to promoting this understanding, my Office could be mandated to prepare a substantive report on the basis of these national views and practices.

Third, deepened engagement with stakeholders must be prioritized.

I have repeatedly emphasized the importance of engaging a range of stakeholders in an inclusive and sustained manner given the unique character of ICTs.

In this connection, stakeholder contributions are particularly important as ICT infrastructure is often developed and managed by private sectors.

These entities can directly support implementation of the normative framework, including through supply chain security of their ICT products.

Given the ongoing limitations of access to Headquarters by non-governmental organizations during the COVID-19 pandemic, it is particularly important that their meaningful participation is safeguarded.

I am encouraged by the Chair’s commitment to systematic, sustained, and substantive engagement with stakeholders.

In this regard, I am pleased to see that tentative dates for informal consultative meetings with stakeholders have already been identified to coincide with each substantive session.

Mr. Chair,

Distinguished delegates,

Combatting peace and security risks in cyberspace necessitates the building of cooperation and trust among States.

In the context of digital global security, trust is a two-way street.
Undermining trust can threaten international peace and security, while building trust supports it.

At the same time, increasing trust between States is an essential ingredient in our efforts to ensure an open, secure, stable, accessible and peaceful cyberspace.

The discussions you launch today through the Open-Ended Working Group are part and parcel of these efforts to build trust.

My Office pledges its full commitment to support all delegations in this endeavour.

I wish you every success with your session this week and I thank you very much for your attention. Thank you, Mr. Chair.