Virtual Event hosted by the Institute for International Cyber Stability


Introductory Remarks by Ms. Izumi Nakamitsu
High Representative for Disarmament Affairs

New York (Virtual Event)
9 June 2020
Her Excellency President Kersti Kaljulaid,
Ambassador Jürg Lauber, Chair of the Open-ended Working Group,
Ambassador Guilherme Patriota, Chair of the Group of Governmental Experts,
Fellow panelists,
Mr. Jim Lewis,
Ladies and gentlemen,

Thank you for the opportunity today to discuss the issue: “Deciding on the Rules of the Road for Cyberspace: The Who, What, Where, When, How”. A very interesting title. I would like to particularly express my appreciation to the Institute for International Cyber Stability and Dr. Catherine Lotrionte for hosting this event.

This issue of international cyber security is particularly timely. The two ongoing intergovernmental processes at the United Nations, as well as consideration of this topic at the recent Arria-Formula meeting of the UN Security Council, organized by Estonia, demonstrates the high international interest in this issue. And cyber security is only made more relevant in light of the COVID-19 pandemic. The pandemic has been moving us towards increased technological innovation and online collaboration. Many would agree also that digital connectivity will be key to our recovery in the post-COVID era.

However, associated cybercrime is also on the rise. Over 300,000 suspicious COVID-19 related websites have been created in March alone. Half a million hacked video conferencing account details are being sold on the dark web. Even more worrying are reports of attacks against healthcare organizations and medical research facilities worldwide. UN Secretary-General António Guterres called on the international community to “do more to prevent and end cyberattacks on critical civilian infrastructure, including healthcare facilities.”

As an introduction to today’s panel discussion, please allow me to focus on 3 points: First, the foundational normative framework that guides our use of ICTs; second, the current processes in the UN to further develop and take the framework forward; and finally, I would like to reflect on the road ahead, both in terms of implementing the nascent global normative framework and beyond.

1 https://twitter.com/antonioguterres/status/1267130273143103493
1. The foundational framework that guides States use of ICTs

The topic of ICTs in international security is not new in the United Nations. It has been on the agenda of Member States since 1998, but the real impetus came with the establishment of the UN Group of Governmental Experts or “GGE”, which convened in five iterations since 2004. A sixth GGE’s work is currently ongoing.

The previous GGEs have cumulatively developed a suite of elements such as that international law, in particular the UN Charter, applies to the use of ICTs; practical confidence-building and capacity-building measures for fostering peace and stability in the digital sphere; and 11 voluntary non-binding norms of responsible State behaviour in the use of ICTs.

These elements do not stand alone, but reinforce each other. For instance, the voluntary norms complement binding commitments under international law, and capacity-building helps build capabilities to implement both confidence-building measures and norms.

In 2015, the General Assembly adopted a consensus resolution which called upon States to be guided in their use of ICTs by the 2015 GGE report. The elements in the report thus provide the global community with an accepted foundation and nascent “normative framework” from which to promote stability in cyberspace.

The elements of this framework are universally accepted and therefore must not be rolled-back. But it is also important to acknowledge that as more countries join in the conversation, room must be made for their needs and priorities, which, in the fast-paced digital realm, may not be exactly the same as 5 years ago.

This brings me to my next point on current inter-governmental processes that are in place to take forward the normative framework.
2. **Ongoing UN cyber processes to further develop and take the framework forward**

As has already mentioned, in 2018, two UN processes, an Open-ended Working Group or “OEWG” open to all Member States, and a Group of Governmental Experts comprising 25 experts working in their individual capacities, were established to take forward the issue of the use of ICTs and international security.

I am very heartened by the substantive and collaborative engagement of many States so far at the OEWG, and also with the GGE through informal consultations of the whole UN membership and regional consultations.

It is clear that an increasing number of States are beginning to recognize the urgency of the issue of ICTs and international security and are committing themselves to action. Greater awareness, recognition and acceptance of the normative framework is growing globally.

Many of these States are engaging for the first time on this issue and are therefore bringing fresh perspectives to the discussions. I am hopeful that this will enable both Groups to build on agreed elements but also take forward the global normative framework in exciting new ways.

In terms of how the foundational normative framework is being taken forward, I believe it is also important to highlight the work done by many regional bodies whether in subscribing to the 11 voluntary, non-binding norms recommended in the 2015 GGE report or to take forward confidence and capacity building measures based on the GGE reports.

I am also encouraged by the continued engagement of private sector, non-governmental organizations and academia, not only on the framework of the ICTs in the context of international security, but also on broader digital issues within the United Nations. In the coming weeks, the Secretary-General will be issuing his Roadmap for Digital Cooperation, and I hope that States and all other stakeholders will continue to actively engage with the United Nations on its implementation.
Ladies and Gentlemen,

Let me conclude by remarks by providing some reflections on the road ahead on these two processes and beyond.

3. The road ahead – implementation of the global framework and beyond

There remains much work to be done through the inter-governmental processes to promote a stable and peaceful ICT environment. The roadmap for this must include efforts to cultivate truly inclusive partnerships, to promote common understandings on key issues and to improve our collective capacity-building efforts and methodology.

I should highlight that as the OEWG and the GGE are both at a critical time in their work, expectations of the international community are high. However, I have full faith in the wisdom and ability of the Chairs of both processes to steer us towards positive outcomes. At the same time, we need to also collectively think outside of the box to ensure cyber stability for the future that not only within the UN processes but also beyond.

For instance, there has been a wonderful “explosion” of important forums around the world for discussing cyber security. Could we do more to harmonize these different fora in which ICT issues are discussed? Or should we be focusing more on engaging young people to better find out what they want in the cyberspace they are inventing but will also inherit?

I don’t have the answers, but as I conclude my brief remarks, I would like to pose the question to encourage discussion both today – taking advantage of the expertise present here.

UN Secretary-General Guterres has said that we need to overcome the digital, social, and political divides in cyberspace in order to achieve “one world, one net, one vision.” Let’s together rise to this challenge.

I thank you very much.