UNODA United Nations Office for Disarmament Affairs

Opening remarks of the High Representative for Disarmament Affairs at the UNIDIR Cyber Stability Conference 2019

New York

6 June 2019

Excellencies,

Distinguished delegates,

Ladies and gentlemen,

Before I start, I would like to thank UNIDIR – Kerstin Vignard and her team – for organizing this event. Today's theme is an excellent one because strengthening global engagement for global cyber stability is more important than ever in our digitally connected world, which brings its own challenges.

Critical infrastructure, such as electrical grids and nuclear facilities that are connected through cyber technologies, make for potentially vulnerable targets.

Malicious acts using cybermeans, as well as the challenges of attribution in cyberspace are undermining trust between States.

We need to work together to address these mounting threats.

The organizational session of the Open-ended Working Group on international ICT security concluded successfully on Monday, and we are about to start the work of the GGE, with regional consultations. Today, States must begin to prepare in earnest for the work that lies ahead.

There are at least three key issues that I believe will be critical to our work going forward.

One: Building on past work;
Two: building a strategic vision for global cyber stability; and
Three: inclusion of all relevant stakeholders.

First, building on past work.

As States begin their deliberations, it is important to recall that they are not starting from a blank slate. This is a view that many States expressed during the organizational meeting.

Both the Open-ended Working Group and the new Group of Governmental Experts are building on the work of five previous GGEs that have been established since 2004.

I believe that the reports of these Groups cumulatively provide us with a nascent normative framework for addressing:

- Existing and emerging cyber threats;
- How international law applies in the use of ICTs;
- Voluntary norms of responsible State behavior; and
- A comprehensive set of measures for confidence-building and capacity-building.

As we head into the substantive work of both the Open-ended Working Group and the GGE, I encourage all States to ensure that they are well-versed in these building blocks for the work ahead.

I welcome events such as today's, and also those organized by Australia and Canada last week, which seek to build awareness and the understanding of all States, enhancing their ability to participate.

For our part, ODA, with the support of the Cyber Security Agency of Singapore, has developed a training course that aims to provide a clear and factual understanding of the GGE's previous reports.

This training course can be used both online and in the classroom. We will hold the first training in New York in early summer, ahead of the first session of the Open-ended Working Group.

Some 50 delegates have already signed up, including at Ambassadorial level, and I hope all of you will take advantage of this opportunity.

The second point I would like to make is about the need to collectively forge a vision for what we want to achieve in the digital environment.

On the process side, I am encouraged by the many delegations who have come to me to discuss how to ensure complementarity between the Open-ended Working Group and the Group of Governmental Experts.

I understand that there is already general agreement that the Open-ended Working Group could focus on confidence-building measures, and issues of implementation and capacity-building, while the Group of Governmental Experts can focus on more technical issues.

I am encouraged by the fact that so many States are already thinking ahead. It makes me feel okay to ask: what comes next?

Should we already start thinking about how we can collectively ensure cyber stability for the future, after the GGE ends in 2021?

This could possibly entail harmonizing the different fora in which ICT issues are discussed, or it could be thinking how to engage young people to better consider what they want in the cyberspace they will inherit.

I don’t have the answers, but I have many questions that I would like to start to pose. I encourage active, candid but sincere discussions today, and in many future opportunities ahead.

My final point today is the need for inclusivity including through a multi-stakeholder engagement.

I am glad to see on the agenda today there will be ample opportunity to discuss how public and private sector can better work together in building cyber stability.

A recent study has shown that 90 percent of security incidents result from exploits against defects in software. To address this, we need the help of software developers, engineers and companies.

Recent initiatives on cyber security that come from the private sector, such as the Cybersecurity Tech Accord, the Charter of Trust and Kaspersky’s Global Transparency initiative, demonstrate the commitment of the private sector to security in cyberspace.

I believe that these are very promising developments, which I hope will form a key pillar in fostering responsibility in the development and use of ICT products and services.

Importantly, these principles agreed to by industry in many respects accord with the voluntary norms endorsed by the General Assembly.

One example is the voluntary norm on ensuring the integrity of the supply chain, which is reflected in the Tech Accord’s commitment to protect against tampering with, and exploitation of, technology products and services.

And the norm on protecting critical infrastructure from ICT threats is reflected in the Charter of Trust’s commitment to establish mandatory independent third-party certifications for critical infrastructure.

Under the Open-ended Working Group process, States and the private sector have the opportunity to come together for the first time in a UN process on international peace and security to take forward multi-stakeholder engagement.

Likewise, under the regional consultations of the Group of Governmental Experts, private sector, academia and civil society will also be invited to engage in UN processes.

But let me stress that “Multistakeholder approach” should not just be a catchphrase. We need the public and private sector, together with civil society and academia, to work earnestly and collaboratively towards our mutual goal of cyber stability.

To conclude, let me say how heartened I am by the broad interest from States, industry, civil society and academia in this important topic, as demonstrated by all who are in the room today.

As always, the UN Office for Disarmament Affairs stands ready to both support and to work with you on this important endeavor.

As you engage in deeper discussions today and hear new ideas from experts from various sectors, I hope creative solutions will come to light. I wish you fruitful discussions ahead.

Thank you.