Opening Remarks by Ms. Izumi Nakamitsu, High Representative for Disarmament Affairs, at the High-Level Event on Cyber Security, hosted by the Prime Minister of Bangladesh

Ms. Izumi Nakamitsu  
High Representative for Disarmament Affairs  
United Nations

New York  
25 September 2018
Her Excellency Prime Minister Hasina,
His Excellency Foreign Minister Balakrishnan,
His Excellency Deputy Foreign Minister Teesalau,
His Excellency Ambassador Otaka,
Excellencies,
Distinguished delegates,
Ladies and Gentlemen,

It is a great pleasure to be with you today.

Digital technology is rapidly reshaping our global society. It touches every aspect of our lives, from the way we communicate, how we do business, to how we organize the critical infrastructure on which we are incredibly dependent.

I am glad that today we are joined by leaders from around the world to discuss this issue at the highest political levels.

Excellencies,
Ladies and Gentlemen,

While we enjoy the benefits of technologies everyday, we are also witnessing a disturbing trend in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These incidents have crippled critical infrastructure, disrupted essential services and undermined public trust in ICT technologies. They have affected many sectors of our societies, putting at risk health systems, the financial sector and electric grids.

Major cyberattacks include one in which an entire country was taken offline due to a “botnet attack” that shut the system down by overwhelming it with traffic.

More concerning still, a recent cyberattack has affected around 200,000 systems in over 150 countries, disrupting the functioning of hospitals. Patient records and medical equipment were reportedly affected, potentially compromising the ability of the hospitals to take care of the ill and injured.

I highlight these particular incidents to illustrate the increasing severity and destabilizing effects of some cyberattacks. They pose profound risks to all States and potentially harm international peace and security.

This is why cybersecurity has become a top priority of the UN Secretary-General, as mentioned in his speech to the General Assembly today. He has pursued two separate tracks.
In May of this year, he launched his comprehensive agenda for disarmament, entitled “Securing our Common Future”. One of the agenda’s three priority areas is “disarmament for future generations”, which encompasses ensuring a peaceful cyberspace.

The Secretary-General has also established a High-level Panel on Digital Cooperation, which is meeting face-to-face for the first time right now. This new Panel aims to raise awareness about the transformative impact of digital technologies across society and the economy, and to contribute to the broader public debate on how to ensure a safe and inclusive digital future for all.

Cyber threats cannot be addressed by technical solutions alone. Indeed, to ensure an open, secure, stable, accessible and peaceful ICT environment. There is a need for a normative framework – agreed to by States – on what should or should not be done in the use of ICTs.

Many of you may already be familiar with the work of the UN Group of Governmental Experts on the use of ICT, which has convened in five iterations since 2004. Their mandate has been to study existing and potential threats in the ICT environment and possible cooperative measures to address them, with a view to promoting common understandings.

Taken together, these Groups have reached success in agreeing that international law applies to the use of ICTs and, in particular that the UN Charter applies in its entirety. The Group also recommended practical confidence building and capacity measures for fostering peace in cyberspace.

One key achievement that I would like to highlight is how in 2015, the Group of Governmental Experts was able to forge 11 voluntary non-binding norms of responsible State behaviour.

All Member States of the United Nations agreed to be guided by these norms, which should inform their policies and decision-making processes in the use of ICTs.

What do these 11 norms aim to do?

First of all, these norms set out the values that are most important in responsible State behaviour in cyberspace, taking reference from international law. These norms require, for instance, States to respect human rights in the use of ICTs and to not allow their territory to be used for internationally wrongful acts.

Secondly, these norms are operational in nature and require that States put in place processes and procedures to ensure, for example, cooperation to prosecute terrorist and criminal use of ICTs and that measures are put in place to protect critical infrastructure.
Excellencies,
Ladies and Gentlemen,

While these 11 norms aim to provide a comprehensive framework to guide State behaviour in cyberspace, they are only the beginning for further, more detailed development and elaborations. They will also have limited value unless all States are able to translate them into concrete action.

Although States bear primary responsibility for their cybersecurity, some States may lack the capacity to implement these norms. This could leave their citizens and critical infrastructure vulnerable. It could also make the country an unwitting haven for malicious actors. Therefore, International cooperation and assistance is crucial to support States in their efforts to create and maintain a secure cyberspace.

In this regard, The UN Office for Disarmament Affairs stands ready to assist States to build their cyber capacities. For example, in partnership with Singapore, our Office is developing an e-learning initiative. This initiative aims to provide States, researchers and students with a greater understanding of how the use of ICT affects international security and how the international community is addressing these issues.

Our Office is also at the early stages of developing a norms implementation toolkit to provide model policy, lessons learned and checklists that will assist States to implement the 11 norms.

These are but some examples of the initiatives being undertaken on capacity-building. There are many others. Today we will have the opportunity to hear from the Adviser to the Prime Minister on Information and Communication Technology Affairs of Bangladesh; from the Adviser to the Prime Minister on Power, Energy and Mineral Resources of Bangladesh; from the UN Office for Information and Communications Technology, OICT; and from the civil society organization, ICT4Peace, on their perspectives and initiatives on capacity-building.

Additionally, we will hear from an industry representative about the work undertaken by Microsoft to support norms building among industry partners.

Excellencies,

Ladies and gentlemen,

The normative framework to ensure the use of ICTs for peaceful purposes is being actively discussed by States. In the coming months and years, other Group of Governmental Experts may be established again to discuss the issue further.

However, let us remember we already have today an existing framework which includes 11 norms of responsible State behaviour to guide us in the use of ICTs. In this context
First, is the importance of multilateralism. Given the nature of the challenges in front of us, no single government will be able to find an effective solution. UN Member States have to work together to identify key issues and to implement the norms to ensure peaceful and stable cyberspace.

Second is the importance of multi-stakeholder approach. No one knows the “ins” and “outs” of cyber security issues better than industry actors and researchers who are confronted with them on a daily basis.

We therefore need to do much better collectively in the area of public-private sector cooperation. While States have a primary responsibility for maintaining a secure and peaceful ICT environment, the private sector, as well as academia and civil society have a central role to play.

The third is the importance of urgency of our work together, and the need for creative, non-traditional and multi-faceted approaches in working together. You will all agree that we cannot wait until a “Titanic moment” or major catastrophe to happen before taking actions. On the need to be more creative, you will also agree that there is no single action or solution to the complex challenges. We have to continue to work on international norm development, implementation of those norms, capacity building to equip governments with better cyber defense capabilities, legislative frameworks and sound polities, perhaps achieving industry standardization, education and training of young scientists and engineers for responsible innovation and application of technologies, and so on. We are fully aware that a traditional international negotiation will not suffice in achieving security and stability in cyberspace.

Together with governments, industry, academia, civil society and individuals, it is my hope that we can continue to strengthen a culture of collaboration and international cooperation and assistance in order to forge an open, secure, stable, accessible and peaceful cyberspace.

Thank you.