Opening Remarks at the
2018 Singapore International Cyber Week

by

Izumi Nakamitsu

UN Under-Secretary-General and High Representative for Disarmament Affairs

18 September 2018
Singapore
H.E. Deputy Prime Minister Teo Chee Hean

H.E. Minister H. Wiranto

Honorable Ministers
Distinguished delegates
Ladies and Gentlemen

I am honoured to be able to give you my greetings and best wishes on the opening of the 2018 Singapore International Cyber Week (SICW).

Thank you for inviting the United Nations to this important gathering. As you are aware, issues related to international digital cooperation have become one of the top priorities of the United Nations, and to Secretary-General Guterres, as we go through transformative changes in the world which some people call the “Fourth Industrial Revolution”. I very much appreciate the chosen theme for this year’s SICW, “Forging a Trusted and Open Cyberspace”.

Trust and openness are the foundation of every good relationship, whether personal relationships, business partnerships or good relationships between States in the bilateral or multilateral contexts.

The Internet of Things or what some are now referring to as the “Internet of Everything” and its interconnection with cyberspace means that trust and openness need to be fostered on various levels and across many different relationships in order to promote an open, secure, stable, accessible and peaceful ICT environment for everyone.
What are the key relationships where trust and openness should be fostered, built and preserved?

First is the trust which the user has to have in the system. They need to be able to trust that the networks they are on and the software they are using will support their need to communicate with the person they intend to communicate with, while ensuring the privacy they expect to maintain. There also needs to be trust in the security and integrity of their data.

In the same vein, the user needs to trust that IT service providers will ensure the security of their products and services.

Second is the relationships between individual citizens, the private sector and their governments. Among those stakeholders, trust and openness in the policy-making process is key.

It is important for citizens to be able to trust that their government will protect their interests in cyberspace, while also striking the right balance between national security and individual rights and privacy.

The private sector and governments need to work together to ensure transparency and openness, inclusiveness, shared responsibility, and accountability, in developing policies and solving common Internet issues.

Third and finally, I would like to particularly stress the importance of State-to-State relationships. The frequency and severity of ICT incidents, together with the complexity of attribution, urgently require that we work together to re-establish trust between States in cyberspace.
Experts point out that cyber risks are increasingly posed by transnational criminal organizations with sophisticated technical capabilities, including possibly with the consent or support from a State, rather than lone individual hackers. Cyberattacks from such perpetrators can pose implications for national security. International cooperation and multilateral efforts will be necessary to address these threats.

At the UN, Member States started discussions on cyber security in 1998, when only 2.5% of humankind were connected to the internet. Since 2004, five Groups of Governmental Experts, or GGEs, have studied how to deal with the threats posed by the use of ICTs in the context of international security.

They have provided us with a common understanding on the application of international law in the use of ICTs, recommended 11 voluntary, non-binding norms on responsible State behaviour and have also recommended practical measures for confidence-building and capacity-building with an emphasis on dialogue, transparency, information sharing and cooperation and assistance.

The 11 norms aim to address a range of issues including international cooperation, respect for human rights and the protection of critical infrastructure.

In 2015, the UN General Assembly adopted a resolution [70/237] by consensus in which it “calls upon Member States to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts.”

The recommendations of the 2015 GGE report should inform and guide the policies and decisions of UN Member States in the use of ICTs.

Discussions on a normative framework to ensure the use of ICTs for peaceful purposes will no doubt continue to evolve. But let us remember that you already
have a solid basis upon which you can build your efforts of increasing openness, strengthening trust and building further norms for a more secure cyberspace. The first step is to start implementing the norms and measures that all governments have already agreed, and to take concrete steps to strengthen cooperation at the regional and global levels.

The United Nations stands ready to work with you and to support you in the joint efforts of forging a trusted and open cyberspace.

I am looking forward to engaging with many of you in the next few days.

Thank you.