Japan-US Digital and Cyber Dialogue organized by Columbia University, Keio University & The Japan Society

“Ensuring Collaboration in a Time of Change”

Keynote Speech by Ms. Izumi Nakamitsu
High Representative for Disarmament Affairs

New York (Virtual Event)
28 May 2020
Professor Murai,
Dr. Walker,
Dean Janow,
Ladies and gentlemen,

Thank you for this opportunity to speak today. I would like to express my appreciation to Keio University, Columbia University and the Japan Society for organizing this event. I want to begin by expressing my hope that you and your loved ones are in good health and spirits under these difficult circumstances.

Please allow me to share a few thoughts on the work being done in the United Nations to address cyber threats; provide an overview of United Nations intergovernmental processes; and highlight the important role of all stakeholders in our common efforts to secure the cyber environment.

But before I do so, I would like to briefly touch on what is naturally on all of our minds – the current health crisis and its implications on cybersecurity.

**COVID-19 exacerbating existing vulnerabilities**

Since the advent of the COVID-19 pandemic, the rapid, large scale adoption of digital technologies is really transforming how we do business, and has prompted innovative new ways to collaborate online. I feel as if I am living now in a virtual world, moving from e-mail to text to e-mail, and from one online discussion to the next. By the way, this is the third online event I am participating today!

Previously, we already relied heavily on ICTs, but the current pandemic has greatly exacerbated this dependency. It has also expanded the attack surface, which can be exploited by malicious actors, unfortunately.

Indeed, our increasing use of ICTs during the crisis is being accompanied by an enormous spike in cyber incidents. Reports indicate that spear phishing attacks have risen 667%
between February and April this year. Furthermore, over 300,000 suspicious COVID-19 related websites have been created between January and March of this year.

Even more worrisome have been the mounting malware campaigns against hospitals, medical research facilities and other critical institutions over the past few months. The World Health Organization (WHO), for example, reported experiencing more than five times the number of cyber-attacks than in the same period last year.

These incidents are compounding people’s already widespread sense of insecurity around their health, livelihoods and future.

The United Nations Secretary-General António Guterres has drawn attention to cyberattacks on healthcare facilities during the COVID-19 pandemic. He called on the international community to prevent and end such attacks on critical infrastructure, which can indeed cause severe harm to civilians.

I am glad that the challenges facing us also give further impetus to multilateral efforts and international cooperation to ensure that people can enjoy the benefits of a trustworthy and secure digital space – especially now that it is most needed.

**The United Nations’ efforts in promoting a more peaceful ICT-environment**

Ladies and gentlemen,

Turning to the work of the United Nations, well before the current crisis, Secretary-General Guterres has already stressed that in cyberspace we collectively face the triune risks of a digital divide, a social divide and also a political divide.

This is why he has made cybersecurity a priority. He established an independent High-Level Panel on Digital Cooperation, co-chaired by Melinda Gates and Jack Ma. The Panel’s report contains proposals on how to harness key opportunities and address the challenges facing us

---

1 https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/
2 https://transparencyreport.google.com/safe-browsing/overview
in the digital sphere. A roadmap for the implementation of these recommendations will be released very soon.

Furthermore, the Secretary-General prioritized UN efforts to promote the peaceful use of ICTs particularly in the context of international security. In his Agenda for Disarmament, he made a commitment to work with Member States to foster a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace.

Because, very unfortunately, such a culture is not a given.

A number of States are developing ICT capabilities which can be used to carry out malicious acts. At the same time, beyond COVID-19-related attacks, other cyber attacks by State and non-State actors against ICT-dependent infrastructure continue to be a major concern. Critical infrastructure such as electric grids and financial systems have been targeted in such attacks, and the WannaCry Ransomware of 2017 affected computer systems across 150 countries, compromising equipment and care for patients in hospitals, as we all know.

Although no loss of life has been reported as yet as directly resulting from a cyber-attack, such incidents bring with them a risk of misperception, miscalculation and, ultimately, unintended escalation of tension between States.

United Nations processes

Ladies and gentlemen,

Key efforts have also been made on cyber security under United Nations processes. As you are no doubt all aware, five Groups of Governmental Experts, have been established since 2004. These Groups have reached success in agreeing that international law, in particular the UN Charter, applies to the use of ICTs. They have also recommended practical confidence-building and capacity-building measures for fostering peace and stability in the digital sphere. The 2015 Group was able to recommend 11 voluntary, non-binding norms of responsible State behaviour in the use of ICTs, which were accepted by all Member States in the General Assembly.
The General Assembly adopted a resolution calling on all States to be guided in their use of ICTs by the 2015 Group’s report. This gives the global community an agreed “normative framework” or *acquis* from which to promote stability in cyberspace.

In 2018, two new Groups have been established under the United Nations – a new Group of Governmental Experts comprised of 25 individuals working in their individual capacity, and an Open-ended Working Group, open to all Member States, to build upon this framework.

The 2015 norms and other measures are universally accepted and must not be rolled-back in the new processes. But 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 the same as 5 years ago when the 11 norms were endorsed. The expert process also foresaw that new norms may need to be developed over time. I hope that there will be space in the discussions, under the Open-ended Working Group in particular, for States to agree to further elaborate existing norms.

**Inclusivity and multi-stakeholder approaches**

Ladies and gentlemen,

The United Nations Member States and the Secretary-General are committing to promote a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace. But we cannot do it alone.

While States carry primary responsibility for maintaining international security, ICTs are an integral part of our societies and other stakeholders have a key role and interest, as well as responsibility, in securing cyberspace.

Perspectives from the private sector, civil society and academia are needed to contribute a unique and important part of the collective solution to cybersecurity that the international community is seeking.

Last year, the Open-ended Working Group held a historic meeting with all stakeholders to consider cyber issues in the context of peace and security. More than 100 stakeholders from
the private sector, civil society and academia joined over 114 States in a rich discussion that received very positive feedback.

The expert process, on its part, has held consultations with regional organizations as well as the wider membership. These meetings have also been very well received by the Member States of the United Nations.

**Conclusion**
Allow me to end my remarks by returning to issue of the COVID-19 pandemic, this time to highlight that there are key analogies between the health pandemic and the threats that we face in the digital world. First, both these threats are not easily seen with the naked eye. With COVID-19, as we now know, there are not always visible symptoms of the disease. Likewise, in an ICT incident, you may not be able to tell if malicious activity is happening in your network.

Secondly, COVID-19 and digital threats both present us with challenges that have no borders. One country’s capacity and decision to act impacts those of other countries around the world.

Finally, and above all, if there is one take away from the current COVID-19 crisis, it is that more than ever, we need to take concerted, coordinated, multi-stakeholder action. We can only beat the pandemic, and we can only effectively address the threats facing us from the ICT environment, if we do so collectively by sharing information, providing mutual assistance and raising each other’s capacities.

I encourage all stakeholders from the private sector, civil society and academia to rise up to the challenge to work together with States to address global digital challenges, so that we can all take forward the goal of an open, secure, stable, accessible and peaceful ICT environment.

Thank you.