Keynote Remarks at Turtle Bay Security Roundtable

“Cybersecurity: A View from Private Industry”

Izumi Nakamitsu, UN High Representative for Disarmament Affairs

New York
6 September 2019
His Excellency Ambassador Koro Bessho,

Distinguished speakers and delegates,

Ladies and gentlemen,

Let me begin by thanking Ambassador Bessho and the Permanent Mission of Japan, and the Stimson Center for inviting me to speak today and for organizing this next iteration of the Turtle Bay Security Roundtable series. The series has now produced several valuable and thought-provoking events including on forward-leaning topics related to international peace and security, disarmament and new technologies. These are not yet topics being discussed across the road in intergovernmental forums, so, it has been useful to have one like this Turtle Bay Roundtable.

Today’s topic is an exception. Issues related to cybersecurity are increasingly of concern to Member States, but also other actors, such as the private sector. Today’s roundtable is particularly timely, as the Open-ended Working Group on ICTs in the international security context starts its substantive work next week.

And another intergovernmental process, a Group of Governmental Experts on advancing responsible State behavior in cyberspace in the context of international security, will commence its work at the global level in December.

International and intergovernmental solutions to issues related to cybersecurity are vital. The nature of the challenges confronting us on cybersecurity means that no single government will be able to find an effective solution.
It also means that while States have primary responsibility for maintaining a secure and peaceful ICT environment, the private sector, as well as academia and civil society also have a central role to play. The term “multistakeholder approach” is a common catch-phrase that we hear with increasing frequency, but in reality, there is still a lot of work to be done to make such approaches effective, especially at the UN.

I am convinced, nevertheless, that effective international “norm making and operationalization” in today’s world in general has to include comprehensive and multifaceted efforts in the traditional intergovernmental negotiations, as well as in developing international private sector self-regulations standards, code of conduct and best practices for companies and even individual citizens. And we need to think strategically about how these instruments should relate to each other.

It is therefore clear to me that UN Member States need to work together with all stakeholders to identify key issues and to operationalize those norms that will ensure peaceful and stable cyberspace.

Allow me today to focus on three points related to creating a more inclusive approach to international cyber security, particularly public-private relationships.

First, the need for trust.

The world’s interconnectedness in the digital sphere requires that trust and openness is fostered on many levels and across many different relationships. Such trust and transparency is central to promoting an open, secure, stable, accessible and peaceful ICT environment for everyone.

The frequency and severity of ICT incidents, together with the complexity of attributing the source of those incidents, is undermining this trust and posing significant risks to international peace and security.

As the two intergovernmental processes commence their work, what I am sure occupies all our thoughts is how to build the much-needed trust between States in the digital environment.

However, there is also another form of trust central to our digitally-driven world.
That is the trust between the public and private sectors. Private companies must have the trust that their government will protect their interests in cyberspace, while also striking the right balance between national security and privacy and, importantly, the freedom to innovate. Private sector needs to have trust that working together with governments to strengthen and implement norms will be good for their business.

Such trust lies at the core of public-private sector cooperation, whether it be information sharing, threat analysis or development of policies to solve common ICT-related concerns. Without this, it will be a challenge to move forward collectively.

And, in this context, by ‘collectively’, I mean the involvement of all relevant actors.

My second point relates to the need to find concrete synergies to facilitate public-private sector cooperation.

It is clear that private corporations and companies are willing to engage with States for a safer and more secure cyberspace. In recent years, many excellent private-sector-led cyber initiatives have been established such as the Cybersecurity Tech Accord led by Microsoft, the Charter of Trust led by Siemens and the Munich Security Conference, and Kaspersky Lab’s Global Transparency Initiative.

Most recently, the Paris Call for Trust and Security in Cyberspace, launched in November last year, brought together industry, States, NGOs and academia in a commitment to nine Principles for cybersecurity. These Principles cover a range of issues from developing ways to prevent the proliferation of malicious ICT tools and practices, to the promotion of widespread acceptance and operationalization of international norms for responsible behavior, as well as confidence-building measures for cyberspace.

It is important to stress that these principles agreed to by industry and the eleven voluntary norms of responsible State behavior, developed through UN Groups of Governmental Experts and affirmed by the General Assembly, are mutually-reinforcing.

For example, the norm to cooperate in developing and applying measures to increase stability and security in the use of ICTs. This is reflected in the Tech Accord’s commitment to support civil society, governments and international organizations in cybersecurity and the Charter of Trust’s principle to promote multilateral collaborations in regulation and standardization.
The norm of ensuring the integrity of the supply chain is reflected in the Tech Accord’s commitment to protect against tampering with, and exploitation of, technology products and services.

The norm of 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.

And these are just a few examples. I believe that a commitment by industry and other non-governmental actors to responsible innovation reinforces States’ commitment to adhere to norms of responsible behavior. I also have no doubt that more synergies will be found going forward. And it is in finding these synergies that we move from discussion to action.

From 2-4 December this year, the Open-ended Working Group on the use of ICTs in international security will hold intersessional consultative meetings with “business, non-governmental organizations and academia”. It is my sincere hope that all interested private sector, non-governmental organizations and academia will join in that much needed conversation with States, where collective discussions on cyber issues in the context of peace and security will take place for the first time under the auspices of the UN.

This brings me to my third and final point, which is a question I would like to ask us all: Looking ahead, do we need to consider a more coherent framework for public-private sector cooperation?

I get encouraged when I see how the private sector entities in different parts of the world are mainstreaming the Sustainable Development Goals into their businesses. What was born out of the UN multilateral negotiations seems to be now owned by various stakeholders beyond governments. These stakeholders also now serve as important actors to push governments to fully implement our universal Goals.

As the international community continues to work on developing and operationalizing international norms, building capacity to equip governments with better cyber security capabilities, and refining legislative frameworks, there are many wonderful initiatives that are blooming and many actors eager to join in the conversation and help with the efforts.
There is still much work that needs to be done to develop a coherent roadmap or guidance for how to collectively implement norms, principles and measures already agreed upon. My question, therefore, is: how can we best find a networked, inclusive solution to the borderless threats that face us in the digital space?

I hope that your discussions today, with their focus on collaboration, information sharing and leveraging the strengths of both the private and public sectors in pursuing our common goal of cybersecurity, will help to shed light on a collective means of securing our common cyber future.

Thank you.