I would like to begin by congratulating Keio University Global Research Institute and The MITRE Corporation for hosting the 10th International Cybersecurity Symposium. It is a great honor and pleasure for me to speak on this occasion. As the Ambassador for Cyber Policy of the Ministry of Foreign Affairs of Japan, I will speak about Japan's cyber diplomacy.

COVID-19 seems to be accelerating the trend of mankind’s increased reliance on Information and Communication Technologies while accentuating the risks and the problems caused by malicious use of such technologies. There is increased reliance on online education and remote working. Diplomats around the world, unable to travel and meet in person, rely more on teleconferencing. Today’s event is online, too. In some countries, remote medicine has become quite common. Smartphone applications are used to contain COVID-19. One such app separates individuals in three categories or three colors, depending on the risk of infection to the virus.

There is a lot of sensitive data and potential damage involved.

It is only natural that there is growing public attention to cyberattacks exploiting vulnerabilities in cybersecurity.

According to statistics from Trend Micro, a leading global security vendor, about 2.97 million users in Japan were victims of phishing attacks during the first half of 2020. That is a 60% increase from the second half of 2019. According to the same source, the number of equipment from which COVID-19 related malware was detected increased from 737 during the January to March period to 5,058 during the April to June period. Almost sevenfold.

A ransomware cyberattack against a university hospital of the Czech Republic last March caused massive damage to its operations, including delay and cessation of surgeries and medical care. In August, 38 companies in Japan reportedly faced unauthorized access to their internal networks, and their VPN codes for remote working infrastructure may have been compromised.

Against this backdrop, it is critical for the international

community to further strengthen efforts to deter and counter cyberattacks and to maintain a free, fair, and secure cyberspace, which is the foundation of vital economic development and creation of new values and cultures, which supports democracy and freedom, and which contributes to international peace and stability.

Japan's Cyber Security Strategy aims to maintain such a cyberspace. As an integral part of the Strategy, Japan’s cyber diplomacy has the same goal and consists of three pillars: “the promotion of the rule of law”, “the promotion of confidence-building measures”, and “capacity building support”.

Let me begin from "the promotion of the rule of law" in cyberspace.

Cyberspace should not be a lawless zone. It should not be the law of the jungle, or the survival of the fittest. Japan is of the view that existing international law applies in cyberspace. This includes the UN Charter in its entirety, including the inherent right of self-defense recognized in Article 51, international humanitarian law, and international human rights law. Based upon the international

customary law of state responsibility, states may take various measures against a cyberattack when it constitutes an internationally wrongful act, to induce the responsible state to comply with its international obligations.

Why is it important to affirm the applicability of international law in cyberspace? International law is in principle about states. States are bound by international law in cyberspace as in the real world and illegal actions should have consequences. International law provides tools for victim states in deterring and countering cyberattacks which may constitute internationally wrongful acts including infringement of state sovereignty, interference, or even armed attack in certain cases. Even in the unfortunate case of ongoing armed conflict, international humanitarian law prohibits cyberattacks against civilian targets.

The Secretary-General of the United Nations has successively established six Groups of Governmental Experts (or GGEs) on cybersecurity at the request of the UN General Assembly. Japan has been present in the last four of them and actively contributed to the

discussions. I am one of the 25 Governmental Experts of the present GGE which started last year. I am an active participant, contributing constructively to the discussions, making use of my experience in international law and international security. It is extremely important that in 2013 and in 2015, the GGEs in their reports affirmed that international law applies in cyberspace. The whole UN General Assembly endorsed the two reports by consensus. Therefore, the affirmation is universal.

Since last year, there is now an Open-ended Working Group (or OEWG) on Cybersecurity within the UN General Assembly. This new framework is open to all UN Member States. At the OEWG in June 2020, 6 countries including Japan expressed grave concern on ongoing cyberattacks against healthcare services and facilities and proposed to consider the medical services and medical facilities as critical infrastructure, like the electricity and water sectors, which should be provided with appropriate protection.

Several UN Security Council Arria Formula meetings have been held on cybersecurity. This May, in an Arria Formula meeting

organized by Estonia, I stated that UN Members should renew their commitments to the purposes and principles of the UN Charter, including respect for human rights, peaceful settlement of disputes, and prohibition of use of force, and that they should explicitly recognize that State responsibility, the inherent right of self-defense as well as international humanitarian law apply in cyberspace, the recognition of which is important for prevention of conflicts and deterrence in cyberspace. I further stated that the Security Council should be ready to act under Chapter 6 or Chapter 7 of the Charter to prevent or to respond to a grave situation involving cyber activities. I believe that it is necessary and appropriate for the Security Council to hold thematic discussions on cybersecurity in preparation of eventual individual cases on which it may be called to act.

Norms of responsible State behavior in cyberspace also play an indispensable role to ensure a stable and predictable cyberspace, complementing existing international law. All UN Members have agreed to a set of eleven norms proposed by the Governmental

Group of Experts in 2015. They must be implemented. Here, I will refer to two concrete norms which are very important when one considers the difficulty to determine who the perpetrator of a cyberattack is.

> According to norm (c), "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;"
>
> According to norm (h), "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;"

Even when a perpetrator state thinks that it can get away with a cyberattack because it cannot be traced, if the victim state indicates that there is malicious activity emanating from the perpetrator's territory and asks for assistance, the former should respond.

In the present GGE, I am strongly supporting the Chair's efforts to build additional layers of common understanding on the agreed content in previous GGE reports. Japan also values highly the OEWG discussions. They contribute to deepening understanding of the past achievements of the GGE by the whole UN membership, and to promoting their implementation.

I must admit though that discussions on international law and norms applicable to cyberspace are becoming difficult. Many countries would like to deepen discussions on how concretely international law applies in cyberspace. The "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" produced and published by an international group of experts can provide an excellent reference to discussions among governments. However, some other countries argue that cyberspace is a new domain where there is a need to create new norms and eventually a new treaty. Japan sees no need at present to start negotiations on a treaty on cybersecurity. Let us use existing rules and implement agreed norms.

Another tool to deter cyberattacks is “public attribution”. It is about publicly expressing condemnation or concern. Public attribution aims to have attackers understand the costs of cyberattacks and dissuade them from conducting them.

In 2017, the Government of Japan issued a Statement by the Press Secretary of MOFA denouncing North Korea’s involvement behind the “WannaCry” incidents. In 2018, another Statement by the Press Secretary was issued to express resolute condemnation of continuous attacks by a group known as APT10 based in China.

International cooperation on countering cybercrime is also important in promoting a rules based cyberspace. Japan is party to the Budapest Convention on Cybercrime and conducts international investigative cooperation and information sharing based on that treaty and other cooperative frameworks. We call on states who have not done so yet to join the Budapest Convention.

The second pillar of cyber diplomacy is "developing confidence-building measures (CBMs)" in cyberspace. In order to prevent an escalation of tensions in cyberspace caused by miscalculation and

misunderstanding, it is necessary for governments to understand each other's national laws, regulations, policies, strategies, and ideas. To deepen mutual understanding, Japan has held cyber policy consultations and dialogues with 14 countries and regions. In 2019, Japan had bilateral consultations with Australia, the EU, France, India, Russia, and the U.S., and a trilateral dialogue with China and ROK.

Japan has prioritized development of regional cyber CBMs. For example, within the ASEAN Regional Forum (ARF), Japan, together with Singapore and Malaysia as co-chairs, led discussions at inter-sessional meetings on cybersecurity in March 2019, and held an expert level meeting in January 2020. Japan will host the next annual cyber-expert meeting and inter-sessional meetings on cybersecurity.

The ARF has been playing an important role in building confidence among members. Members have agreed to (a) the establishment of a directory of points of contact, (b) sharing of information on national laws, policies, best practices and strategies

as well as rules and regulations, (c) awareness-raising and information sharing on emergency response to security incidents, and (d) organizing workshops on principles of building security in the use of ICTs in the national context.

The final pillar of cyber diplomacy is "cooperation on capacity building," Due to the connected nature of cyberspace, the lack of adequate incident handling capacity in some countries and regions may pose a risk to the entire world.

Japan has been providing capacity building support mainly in ASEAN countries to Computer Security Incident Response Teams (CSIRT) and relevant administrative and investigating agencies. The ASEAN-Japan Cybersecurity Capacity Building Centre was set up in Thailand to advance the skills of cybersecurity officials and critical information infrastructure operators in ASEAN. Officials from ASEAN and Japan also hold “Cybersecurity Policy Meetings” to strengthen trust and foster policy coordination. They also conduct joint table-top-exercises and workshops. Japan provides lectures, exercises, facility tours, and other opportunities

to policy advisors, criminal justice practitioners, and others in regions such as Asia, the Middle East, and Africa as part of the JICA's Group and Region-focused Trainings.

Japan also supports the “ASEAN Joint Operations Against Cybercrime” and the “ASEAN Cyber Capacity Development Project”, both conducted by the INTERPOL Global Complex for Innovation (IGCI) through the Japan-ASEAN Integration Fund. Japan will continue to provide strategic and effective assistance through the efforts of the entire government.

I hope that my speech was useful in understanding the importance of rule of law in cyberspace, and Japan’s proactive contribution to international peace and security in cyberspace. In his first press conference, Prime Minister Suga stated his intention to strongly promote Japan’s digital transformation. Under his leadership, Japan will continue to conduct a proactive cyber diplomacy for a free, fair and secure cyberspace.

I thank you for your attention.