Mapping the Future of US-Japan Cybersecurity Cooperation

Abstract and Background

On Thursday September 8, 2022, the US-Japan NEXT Alliance Initiative hosted a bilateral dialogue on mapping the future of US-Japan Cybersecurity Cooperation. The in-person event welcomed around a dozen American and Japanese participants from government departments and think tanks. After introductions, two panelists, Ms. Mihoko Matsubara of NTT and Mr. Taro Hashimoto of CSIS/NTT gave presentations on bilateral cooperation from an international security perspective and from a public-private partnership perspective, respectively. The subsequent group discussion section provided useful insights into both countries' efforts to bolster cybersecurity defenses given the current tumultuous security environment.

This event is the second cybersecurity mapping roundtable dialogue hosted by the NEXT Alliance Initiative. The presentations and participant comments support our project to create a web-based interactive alliance mapping tool to describe how each country organizes itself to defend cyberspace. Central to this project is understanding both countries' cybersecurity operations, how they mitigate risks, and how they collaborate with the private sector and international allies and partners.

Matsubara Presentation Summary

Ms. Mihoko Matsubara, Chief Cybersecurity Strategist at NTT Corporation gave a presentation on US and Japanese cybersecurity cooperation through the lens of recent global events. Russia's war on Ukraine and China's most recent belligerency towards Taiwan in August precipitated change in Japan's cybersecurity defenses and infrastructure.

According to Ms. Matsubara's presentation, Japan received a boost to its efforts in furthering cybersecurity from the serious change in the security environment of the world and recent cybersecurity legislation in Japan. The Act on the Protection of Personal Information (AAPI) is *the* fundamental law on cybersecurity in Japan. Prior to being amended in 2016, AAPI primarily governed personal information for business operators. Since then, the framework established an independent agency called Personal Information Protection Commission (PPC) whose primary responsibility is adjusting policy for personal information protection. The most recent amendment focused on further regulation of cross-border data transfers and came into force in April 2022. During the Tokyo Olympics, officials recorded over 14 million cyber intrusions. The scale of the Olympics cyber intrusions is emblematic of a greater threat facing the country in recent years, as cyberspace becomes a focus for security. These external pressures gave Tokyo the mandate to act in defense of the country's critical infrastructure.

Her presentation then outlined cyber lessons learned from the war in Ukraine. She noted how Russian forces utilized a variety of tactics within cyberspace to both gather intelligence and disrupt Ukrainian critical infrastructure in order to make it challenging for the country to resist. She also noted that despite their efforts, the Russian military seemed to blunder in coordinating cyber and kinetic attacks, a critical error by the Kremlin. Matsubara also profiled lessons from the Chinese military drills towards Taiwan in August. She examined Chinese cyber, information, and electronic warfare tactics targeting Taiwan's morale and government.

Ms. Matsubara then outlined how these recent events impacted Japanese government cybersecurity planning and efforts. She noted accelerated cybersecurity efforts by the Japanese government, (e.g., then Defense Minister Nobuo Kishi's visit to the US Cyber Command in May; Japan Ground Self-Defense Force (JGSDF)'s inaugural multilateral cyber exercise in March that also covered hybrid

warfare; and a broadening of national security awareness into the cyber, electromagnetic, and information domains). Within the SDF, changes include the commencement of a public cyber seminar with US counterparts; JGSDF senior delegation's visit to Ukraine to meet Ukrainian Defense Minister in 2020; furthering of education at the JGSDF Signal School and High School; and the expansion of the Cyber Protection Unit to cover broader areas in Japan. Recent global developments have indeed motivated the Japanese government to develop cybersecurity safeguards in coordination with allies and partners.

Ms. Matsubara's presentation provided invaluable insights to the development of domestic and international Japanese cybersecurity efforts. She concluded her remarks by calling for more in-depth international and domestic communication channels, greater capacity building and a more explicit and cyber focused national security strategy to meet emerging threats to Japan.

Hashimoto Presentation Summary

Mr. Taro Hashimoto, Visiting Fellow (from NTT) for the Japan Chair at the Center for Strategic and International Studies (CSIS) gave a presentation on US-Japan Cybersecurity Cooperation. His remarks covered the functions of Japan's cybersecurity agencies, public/private sector partnerships and how international cooperation contributed to the national efforts to strengthen cyber defenses. He began by identifying Japan's 14 different sectors of critical infrastructure which are mostly owned by the private sector and overseen by various government agencies. They include telecommunications, administration services, finance, logistics, aviation, airport, railroad, water supply, medical care, electric supply, gas supply, chemical industry, credit card and petroleum industry. Coordination with the private sector is handled by National Center of Incident Readiness and Strategy for Cybersecurity (NISC), while protection measures are outlined in a 5th national action plan released in June of 2022. Hashimoto then covered how governmental agencies safeguard critical infrastructure in times of crisis and noted different measures that can be employed, including public/private initiatives for information sharing and analysis and the contents of the Economic Security Promotion Act that was newly enacted this year.

He then pivoted to international engagement and how Tokyo is working with other governments to build cyber resiliency. On US collaboration, he noted the summit in May 2022 that outlined the

progress of the US-Japan Competitiveness and Resilience (CoRe) Partnership. Key components of the partnership improve cybersecurity and critical infrastructure resilience and strengthens collaboration on Open Radio Access Networks (ORAN) telecommunications technology. He also noted the US Japan Cyber Dialogue and the US Japan Policy Cooperation Dialogue on the Internet Economy (IED).

Within the QUAD, he profiled the Joint Leaders' Summit in May 2022 and the Cybersecurity Partnership which advances workforce development, software security, supply chain risk management and critical infrastructure cybersecurity. Finally, he noted industry-led collaborations with various sectors including Information Sharing and Analysis Centers (ISAC) for the IT/Comm sector, financial sector, electric sector, and medical sector.

Mr. Hashimoto's presentation provided invaluable insights to the functionality of Japan's cybersecurity in government and industry, including critical infrastructure sectors. He concluded by suggesting next steps for US Japan bilateral cooperation including greater mutual understanding of cyber functions and roles that are decentralized among government and industry while maintaining a holistic view of cybersecurity. It also includes expanding industry's participation to operationalize the cooperation within and across sectors and building greater information sharing mechanisms with trust and sufficient resources to provide the cybersecurity infrastructure with the means of meeting the challenges and threats that face Japan.

Discussion Summary

The discussion section allowed participants to pose questions to the presenters and each other about US, Japanese and bilateral cybersecurity efforts. An American participant wondered what sectors Japan was particularly concerned about. She noted that the US sees ransomware attacks on utility industries, energy companies and smaller more vulnerable areas like education and healthcare. She wondered if the Japanese had seen attacks on similar areas and what the government could do to support victims collectively. A Japanese participant responded that following the invasion of Ukraine, Japan's financial sector was put on notice to expect cyber intrusion as the government levied sanctions against Russia. Larger Japanese firms bolstered their cyber defenses and stopped paying ransoms, but smaller companies were also targeted. The

Japanese police launched a task force to assist smaller and medium-sized companies confronting economic espionage and ransomware. Adding to that, a Japanese participant commented that the larger sectors like financial and telecom firms are generally capable of withstanding attack, but noted that the vulnerable medical and education sectors are being hit because they are smaller and more numerous (i.e., harder to protect).

Another part of the discussion was compartmentalization, brought up by an American participant citing concerns rooted in the September 11th attacks. She said that what is most needed in cybersecurity defense is leadership. Leaders need to keep people accountable and direct agencies and sectors to cooperate. She noted that cultural obstacles can prevent organizations from sharing information but insisted that they can change. She warned participants to not wait until 3,000 people die (referencing the 9/11 attacks) before fixing things. Regarding Japan's new Digital Agency, she said that it must work on harmonizing security clearance (access) issues and cross-governmental communications. Another participant concurred and added that the Digital Agency is new and small, but there is potential if leadership is counseled in the right direction.

Senior Director Schoff asked an American participant if current initiatives in the US and abroad are able to coordinate with each other (and with private industry) using a single set of standards. The participant responded that her agency stresses leveraging international standards whenever possible, as well as working to enable US standards to be interoperable with nations across the world. She continued, saying that as government initiatives are undertaken there is frequent soliciting of input from public and private entities to ensure that the standards and guidelines are useful and incorporate international perspectives. She also noted that the US contributes to this effort by fostering personal and institutional connections and information sharing.

Senior Director Schoff asked about the JGSDF exercises and how wide the lessons learned there are disseminated throughout the government and other military services. A Japanese and American participant responded that those lessons are not spread far enough, and while the training does a good job identifying challenges, it does not guarantee the proper solution is adopted. The Japanese participant concurred and said that Japan struggles with identifying when and how to move between peace, gray zone and kinetic conflict, in terms of crafting a sufficient response.

An American participant asked about ISAC/CERT and if it is for incident report sharing and if there is a divide in the pre-incident and post-incident on how those two structures share information. A Japanese participant said that the ISAC definition depends on the organization, but in Japan working groups within organizations share threat information and best practices and how to conduct incident response. Another Japanese participant said that ISAC is sector driven and that due to non-disclosure agreements you will hardly ever know what level of information sharing is going on. An American participant noted that the older ISAC/CERTs are best due to the long-standing personal relationships and the trust that has built up. Generally speaking, financial ISAC/CERTS are the best example of this. She then described ISACs as "left of the boom" and CERTS as to the "right of the boom."

An American participant said that there is heightened concern for cybersecurity in Japan and that leadership is important to keep making progress. He encouraged the participating experts to journey to Japan and talk to government officials in a constructive way, taking note of gains made and providing practical advice for further improvement. He continued, saying that a group of knowledgeable people making constructive connections could do a lot in promoting US Japanese cooperation specifically in the cybersecurity domain.

Senior Director Schoff closed the meeting thanking the participants for their presence and important contributions to the alliance mapping project. He said that the NEXT team would do its best to facilitate bilateral communications and coordination in a follow up to this event. He also said that building the network in Washington and Tokyo is vital to encourage an open dialogue in order to face the key challenges both nations face in the cybersecurity landscape. Cybersecurity is becoming an increasingly important part of US and Japanese strategic interests and alliance management. The presentations and discussion session gave the NEXT team a broader perspective to consider. Updates regarding the alliance mapping project for cybersecurity will be published when available.

---

*The **US-Japan NEXT Alliance Initiative** is a forum for bilateral dialogue, networking, and the development of joint recommendations involving a wide range of policy and technical specialists (in and out of government) to stimulate new alliance connections across foreign, security, and technology policy areas. Established by Sasakawa Peace Foundation USA with support from the Nippon Foundation, the goal is to help improve the alliance and how it serves shared interests, preparing it for emerging challenges within an increasingly complex and dynamic geostrategic environment. Launched in 2021, the Initiative includes two overlapping lines of effort: 1) Foreign & Security Policy, and 2) Technology & Innovation Connections. The Initiative is led by Sr. Director Jim Schoff.*
