Mapping the Future of US-Japan Cybersecurity Cooperation: Post Summit Roadmap

Abstract

On May 14, 2024, the US-Japan NEXT Alliance Initiative convened a hybrid bilateral dialogue on the post Biden-Kishida summit cybersecurity agenda. Senior Director Jim Schoff welcomed around 20 American and Japanese specialists to the event from both governments, think tanks, and the private sector. Ms. Mihoko Matsubara (Chief Cybersecurity Strategist at NTT) and Mr. Taro Hashimoto (Visiting Fellow from NTT at the Center for Strategic and International Studies) gave opening presentations that provided an update on the Japanese government's cybersecurity initiatives in a geopolitical context, and how the private sector is changing in light of government guidelines and global challenges. The group then discussed a range of related topics including Internet of Things (IoT) cybersecurity labeling, critical infrastructure protections, and private sector security clearance legislation that passed Japan's Diet in May which covers non-defense related companies for the first time. This was the fifth cybersecurity dialogue hosted by the NEXT Alliance Initiative.

Opening Remarks

Ms. Mihoko Matsubara, Chief Cybersecurity Strategist at NTT, kicked off the event with a presentation that covered bilateral cybersecurity initiatives noted in the Biden-Kishida joint statement. Her presentation walked the participants through the main points covered in the April joint statement: AUKUS Pillar II, North Korea's illicit cyber activities, ICT resilience and critical infrastructure protection, and the security of Taiwan along with Japan's Southwest islands. She noted that although cybersecurity is not central in the Summit documents, it permeates all aspects of recent gains in US-Japan security through these four areas.

She opened by noting that Generative AI was both an opportunity and a threat to security, as it helps to locate vulnerabilities and mitigate burden on cybersecurity professionals, but also provides a means for adversarial actors to breach systems and create phishing messages more easily. On regional issues Matsubara highlighted that as the Kim regime in North Korea continues to make millions via its illicit cyber activities, the US, Japan, and South Korea should continue working jointly to strengthen collective cybersecurity and restrict the flow of illegally acquired funds that support North Korea's nuclear program. She noted a UN Panel of Experts report in March on North Korea sanctions that said 58 suspected DPRK cyberattacks on cryptocurrency related companies between 2017 and 2023 had stolen about $3 billion for the regime.

On Taiwan, she said there is growing concern among the allies of an impending crisis, especially as the Washington Post reported in December 2023 about a number of breaches in US critical infrastructure companies including a water facility in Hawaii, a major west coast port, and an oil and gas pipeline. In addition, in January 2024, the US government announced having disrupted Chinese hacking operations against critical infrastructure targets domestically and against international partners. In the Office of the Director of National Intelligence (ODNI) annual threat assessment of February 2022, the goal of such infiltrations is to deter US military and/or governmental action by impeding decision making, sparking societal panic, and hindering the deployment of US armed forces.

On US governmental strategic responses to this, Matsubara highlighted the words of former NSA Cyber Director Rob Joyce about themes of distraction and disruption in cybersecurity operations. He reportedly said during a roundtable with journalists in March 2024, "They want leadership focused inward and dealing with crises here and not worrying about things overseas." Also, CISA chief Jen Easterly said in a hearing of the House Appropriations Subcommittee on

Homeland Security in April that the findings of the Chinese Volt Typhoon hacking operation were "the tip of the iceberg," as the DHS organization threat-hunts across critical infrastructure sectors. To address concerns, Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology, is implementing a three-part strategy that includes, ensuring critical services have minimum cyber practices in place, focused mitigation through warning and practical steps by CISA, FBI, along with other intel agencies, and discussions with Chinese officials at high levels.

Mr. Taro Hashimoto, Visiting Fellow from NTT at CSIS gave his presentation on how the US-Japan summit's proposed changes to security cooperation would impact the private sector. Hashimoto opened by highlighting key points of the summits' joint statement and fact sheet that outlined the mutual goals of both countries from deepening cooperation on information and cyber security to build resilience in ICT domain, to critical infrastructure protection, AI safety, and mutual recognition on IoT cybersecurity labeling schemes.

The figure below shows the current cybersecurity legislation against the pending changes following a bill that passed the Diet in May of this year. The bill creates a process to extend security clearances to companies that might not have a direct link to defense industrial programs but are part of the nation's critical infrastructure. The previous system only protected national security information for defense, diplomacy, espionage, and terrorism. The expanded system covers economic security information such as cybersecurity and supply chain vulnerabilities. The new security clearance system is meant to serve as a foundation for operational collaboration in cybersecurity. The intention is to expand an interoperable mechanism for US-Japan intel sharing to cover cybersecurity, and prepare industry for new policies, facilities, and people to be cleared.

	New Security Clearance System in Japan	
	Existing system	**What will be additionally included**
Law	Specially Designated Secrets Act	New legislation (Lower House: passed, Upper House: under deliberation)
Information	Important national security information (Defense, diplomacy, espionage, and terrorism)	**Important economic security information (e.g., cybersecurity threat/measures, vulnerabilities in supply chain)**
Types	Top secret, Secret	**Confidential**
Entities	Government, limited scope of private sector	**Broader scope of private sector**

Hashimoto continued, highlighting the key points of the Economic Security Promotion Act that was passed in May 2022 and has been gradually implemented over a two-year period. The law

includes screening of core infrastructure prior to installation and applies to suppliers of components and outsourced entities, covering 200+ core infrastructure owners and operators across 14 sectors. On the implementation of the national security strategy, Hashimoto highlighted the current legislative discussions, including secrecy of communications and the formation of a panel of experts to make recommendations on future bills. He also noted the reinforcement of cyber capabilities, including the expansion of cyber staff throughout the government and the preparation for a new national cybersecurity agency.

Finally, Hashimoto spoke about governmental efforts to implement ACD strategy by enhancing government operational capability, enabling bidirectional public-private collaboration, and starting first with a range of proactive cyber operations. In addition, he highlighted the potential benefit of national-level risk analysis for critical infrastructure cybersecurity and resiliency that both countries could rely on, and a US-Japan joint cyber exercise to include both public and private sectors.

Discussion Summary

During the discussion segment, participants posed questions and comments building upon the presentations. The dialogue centered primarily around two main points, the evolution of Japan's security clearance system, and efforts to enhance mutual recognition of IoT protections and cybersecurity labeling.

Beginning with the security clearance system, an American participant asked if the Japanese government had considered the cost and if there would be proper funding for its effective implementation. To this, a Japanese participant said that one obstacle in terms of cost is, unlike in the US, there is not a wide network of military veterans and former intelligence officers who understand the nuances and value of a clearance system, nor can they staff it. Also, the public remains mostly unaware of why it is needed and what is needed such as sensitive compartmented information facility (SCIF), which makes it difficult to operationalize security clearance. An important step for Japan will be realizing that the security clearance system can be a valuable investment of time and money over time, and not simply a cost of doing business.

One American participant lauded Japan's move to centralize the clearance system effort and acknowledged the difficulty of implementing such a system. He pointed out that even within the US, there is not always reciprocity on clearances and some circumstances require a start from

square one. Another American participant said that the end goal of this effort is an information sharing ecosystem, to which another participant concurred and suggested that perhaps that ecosystem should be the primary goal, while the clearance system acts as an assurance that Japan has the capability and culture of being a part of a secure cyber information sharing space. An American participant noted that the system will probably apply to only a relatively small number of people but broadly distributed across industry, as the cybersecurity piece is viewed as a "must have" for business and critical infrastructure. Employing a few people who can work across sectors under a clearance umbrella should add value for the companies. Another participant cautioned that the Japanese government may be headed towards an overextension of the effort and suggested that perhaps clearances should be rolled out on a small scale where issues could be ironed out first, then built out more broadly from there.

A participant noted that this new system is being implemented to match the US ideal of sole designated authority and thus could overcome the issues surrounding the sharing of sensitive information between the two countries. He continued, saying that although the new system wouldn't be inaugurated with perfect functionality, Japan could work those issues out over time but the cost of doing nothing would be far greater than clearing a few key people. Another participant warned that while this lengthy process of implementation is ongoing, there are organizations that remain vulnerable while waiting for both governments to institute the change. He added that the void in information sharing infrastructure between governments has forced organizations to build their own "point to point" understandings and agreements. These information channels include TLP (Traffic Light Protocol), which is used by both countries' non-profit organizations, where parties agree to information distribution limitations and users are only governed by the legalities of what they can share. Although TLP is not a substitute as a classified information sharing mechanism, a third participant said that it is a popular, information sharing ecosystem due to its accessibility. An "all of the above" information sharing infrastructure including classified material will likely be needed.

An American participant said that on the civilian and critical infrastructure side, IoT cybersecurity labeling is a great initiative, but there may be issues of mutual recognition that would lead to a "lowest common denominator" approach that is below the standard for entry into a market. Another participant asked who on each side is leading the effort on cyber trust labeling and IoT, to which a Japanese participant responded it is the FCC (for the US) and METI (in Japan). A

participant also raised the issue of potential disagreements erupting when market access is at stake. A domestic company could complain that it needed to reach a certain high standard for cybersecurity assurance that another foreign company did not, yet each received the same access due to mutual recognition. Or it could be seen as a bureaucratic tool to limit market access for protectionist reasons. Transparency and objective standards and testing will be necessary.

NEXT Steps

Senior Director Schoff closed the event by thanking the participants for their insightful comments and good discussion. This fifth "mapping the future of alliance cybersecurity" roundtable comes as NEXT continues its effort to map out the US side of the cybersecurity infrastructure landscape, to build its "Alliance Mapping Tool" on the NEXT Alliance Initiative page of the Sasakawa Peace Foundation USA website.

---

*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.*
