Mapping the Future of US-Japan Cybersecurity Cooperation: Japan's Pending Cybersecurity Reforms

Abstract

On Wednesday June 21, 2023, the US-Japan NEXT Alliance Initiative convened a bilateral roundtable dialogue on Japan's pending cybersecurity reforms. Senior Director Jim Schoff welcomed 10 American and Japanese participants to the hybrid event from think tanks, both governments, and the private sector. Mr. Taro Hashimoto, Visiting Fellow at the Center for Strategic and International Studies (CSIS) from NTT gave a presentation on cybersecurity measures within Japan's new national security and defense strategies. The discussion portion of the event covered a range of topics, from bilateral information sharing and possible legal adjustments, to future cooperation and coordination to defend against bad actors. Japan's new National Security Strategy calls for a major restructuring of its National Center for Incident Readiness and Strategy for Cybersecurity (NISC) to coordinate policies more comprehensively and in a centralized manner. The Japanese government is now considering numerous proposals to achieve these reforms through new legislation to be introduced in 2024. The presentation and participant comments support a NEXT project to create a web-based interactive alliance mapping tool to describe how each country organizes itself to defend cyberspace. This was the third cybersecurity mapping roundtable dialogue hosted by the NEXT Alliance Initiative.

Opening Remarks

After introductions, Hashimoto gave a presentation entitled "Cybersecurity in Japan's National Security Strategy." His remarks outlined what he thought were important potential improvements to Japan's cybersecurity capabilities facilitated by three strategic documents released by Japan's government in December 2022. The National Security Strategy, National Defense Strategy, and Defense Buildup Program constitute a landmark shift in the country's security policy in the postwar era. The changes are being implemented at a time when the Japanese government is also advancing its cybersecurity capabilities and collaborating with like-minded countries to collectively defend against malicious actors.

The core of Hashimoto's opening remarks centered on three main areas described in the strategy document: 1) the implementation of "Active Cyber Defense;" 2) restructuring the government's cybersecurity organization to make it more centralized and therefore easier to coordinate; and 3) enhancement of international cooperation with like-minded allies and partners.

Hashimoto first highlighted key references within Japan's National Security Strategy concerning efforts to improve cybersecurity response capabilities by the government. The Strategy notes how responses would improve by establishing mechanisms to assess regularly the systems utilized by government agencies. It also emphasized the continuous enhancement of diplomacy, defense, and intelligence. The government will also promote the development and effective use of human resources by actively adopting cutting-edge concepts and technologies related to cybersecurity at all times. Furthermore, government efforts will become more streamlined and centralized with the establishment of a new National Center for Incident Readiness and Strategy for Cybersecurity (NISC).

One major point that Hashimoto covered was Active Cyber Defense (ACD), which the Strategy describes as a way to eliminate in advance the possibility of serious cyberattacks that may cause national security concerns to the government and critical infrastructure. He outlined three ways that the strategy document suggests the Japanese government can introduce ACD: 1) improving information sharing with the private sector (particularly critical infrastructure); 2) detecting servers and others abused by attackers by utilizing information provided by telecommunications providers; and 3) taking necessary measures for the government to penetrate and neutralize malicious actors

in advance of an attack. However, Hashimoto emphasized that it is important to focus on discussing what Japan will substantially pursue based on the Strategy regardless of whether it is technically in the scope of ACD. As there is no clear definition on ACD (depending on the nation or context), focusing too much on the term itself could cause misunderstanding (e.g., only considering the offensive side of measures) or limit the scope of measures the government can take to respond to a specific incident. He also noted that a number of existing measures can be leveraged to implement the strategy while also investing in novel initiatives. For example, ACD could range from more passive activities, such as information sharing, "tarpits" (servers that purposefully delay network connections), and "honeypots" (virtual traps to lure attackers), to more active and higher impact operations, such as botnet takedowns or white-hat ransomware.

On changes driven by the security documents, Hashimoto noted three areas he expected would change over the coming years. These include how to operationalize public and private partnerships, enhance international cooperation, and update inadequate cyber resources and authorities for government officials.

Hashimoto underscored that implementation of the Strategy would fundamentally enhance the government's cyber capabilities, facilitate operationalizing a public-private partnership through bi-directional cooperation (i.e., each assisting the other), and lead to better collaboration with the international community of like-minded nations for various fields of joint efforts (e.g., information sharing, public attribution, and take-down operations). He suggested that the release of an implementation plan that defines specific measures with roles and responsibilities for the public and private sectors along with a timeline would help stakeholders construct a dialogue on changes to national strategy, while also signaling Japan's commitment and direction domestically and internationally.

Discussion Summary

Japan's Cybersecurity Development

A Japanese government participant followed Hashimoto with his own views about key cybersecurity issues. He began by describing how critical infrastructure and government services are highly vulnerable to cyber-attacks from adversaries, especially North Korea. He shared how in 2022 there were over 230 cases of ransomware cyber-attacks in Japan, marking a dramatic uptick.

Critical industries (e.g., automobile, semi-conductor) have been compromised both in the United States and Japan. The participant advocated for "whole-of-government approaches" on this issue. Secondly, he echoed Hashimoto's recommendation of operationalizing public and private partnerships. He said, "the notion of national security as only a government issue is no longer applicable." Because these attacks frequently go through communications equipment controlled by the private sector, the government should coordinate more on industry-led responses. This is also meant to address what he described as "the sophisticated nature of these attacks." Lastly, the participant addressed Active Cyber Defense. He contrasted current Japanese cybersecurity with US offensive cyber operations, underscoring Japan's commitment to remain defensive, aiming to prevent attacks by utilizing private-sector partnerships and communication data.

A US participant responded with support for a "holistic" governmental response in Japan. He further outlined his "wish list" for the development of the new NISC. He recommended faster sharing and more resilient handling of US classified information with Japanese government entities, namely the Ministry of Foreign Affairs, the Ministry of Defense, the Cabinet Intelligence Research Office, and the Acquisitions Technology Logistics Agency (ATLA) within the Ministry of Defense. Because of Japan's reliance on private contracts in the cyber arena, the government could also foster more unified collaboration between its own agencies and industry contractors (including the handling of classified information). Lastly, the participant recommended flexibility in contracting mechanisms, mainly to handle an increasing frequency of threats and adversarial use of artificial intelligence tools.

The US Side

Building on this, another US participant expressed that challenges faced by the United States and Japan in the cyber sphere are similar, specifically the issue of integrating departments into a centralized strategy. However, he acknowledged that this is a difficult feat amongst numerous entities tasked with cybersecurity, including the US Cybersecurity Infrastructure Security Agency, the Federal Bureau of Investigation, the Office of the National Cyber Director, and others that focus on protecting critical infrastructure but operate within larger agencies, such as the Departments of Energy, Treasury, State, and others. He noted how the US response to cybersecurity issues is frequently "ad-hoc" in style. This improvisation creates challenges in

standardizing inter-agency or intergovernmental collaborations. When asked about US cybersecurity successes and challenges, he emphasized the hardship of scaling up effective cases of coordinated effort. As for successes, he referenced the newly published National Cybersecurity Strategy, accomplishing broad interagency and private industry buy-in for a common approach. The participant saw the US strategy's development and release as progress toward more unified protocols, as well as promoting necessary cyber regulations to protect critical infrastructure.

Legal Considerations

On the topic of Japan's legal mechanisms, a Japanese participant noted that the Japanese Constitution places strict protections for citizens' privacy (e.g., Article 21 guarantees their right to "secrecy of any means of communication"), so the public and private sectors must navigate complicated legal questions when balancing national security needs. Criminal activity is not protected, of course, but there are underlying government challenges at times in how to legally access necessary communication data.

Another Japanese participant added that Japan needs new legal instruments in addition to what is currently available. In addition to strong domestic protections of privacy and confidential communications, Article 9 of the Constitution might also be seen as limiting certain tactics related to Active Cyber Defense. There should be ways to satisfy Constitutional requirements and national security needs, but these legal clarifications will likely take time to sort out.

On the US side, an American participant shed light on how government sectors are looking to shape responses. This includes reauthorizing Section 702 of the Foreign Intelligence Surveillance Act, set to expire at the end of this year, which provides more authority to surveil foreign persons on US networks. The participant also mentioned how the Department of Commerce is exploring regulations on US-based internet infrastructure providers. Goals include increasing awareness of customer requirements and preventing bad actors from misusing networks (i.e., a "know your customer" approach).

Improving US-Japan Collaboration

All participants emphasized a need for more cooperation and standardization for effective information sharing, where both Japan and the US prioritize the sharing of cyber information as

global partners. In addition, a Japanese participant stressed cyber diplomacy's vital role vis-à-vis other nations and international organizations. Japan considers this to include capacity building for developing nations, calling for global standardization in the cyber realm, and continuing these dialogues when participating in international forums (e.g., G7, The Quad, and others).

A US participant endorsed more bilateral information sharing, but he included an emphasis on bi-directional flow. Another US participant wished for stronger lines of US-Japan communication on cyber-related intelligence and cyber policy development. He also urged for real-time, expedient sharing of best practices.

---

*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.*
