22

Japan's Cybersecurity Policies

Mihoko MATSUBARA

Introduction

The period covered in this article begins with the cyberattacks on Japan in 2000, which prompted the country to earnestly engage in enhancing its cybersecurity capabilities, and extends to the cybersecurity threats associated with Russia's invasion of Ukraine in 2022 and ransomware attacks that occurred in the summer of 2023. This paper aims to review the cybersecurity policies and international cooperation that Japan has thus far pursued and examine future policies that Japan is required to develop as the threat landscape has changed.

Pre-Tokyo 2020

The Japanese government was prompted to earnestly engage in enhancing cybersecurity capabilities in January 2000 when cyberattacks defaced the websites of the Science and Technology Agency, the Ministry of Internal Affairs and Communications, and other government agencies. The rapid development of information technologies (IT) made it urgent for the government to take cybersecurity measures and to develop relevant policies. This led to the establishment of the Cabinet Secretariat's Information Security Measures Promotion Office at the end of the following month. The office was reorganized in 2005 as the Cabinet Secretariat's National Information Security Center. In September 2011, Japanese media reported a series of cyberattacks on major Japanese defense contractors: Mitsubishi Heavy Industries, IHI Corporation, and Kawasaki Heavy Industries. These attacks further heightened Japan's concern and interest in cybersecurity.

Against this backdrop, Tokyo was selected to host the 2020 Summer Olympic and Paralympic Games in September 2013. The Olympic and Paralympic Games had been regularly hit by various threat actors because of the global attention they attracted. As both physical security and cybersecurity were indispensable to the successful hosting of the Games, such awareness further reinforced Japan's commitment to strengthening its cybersecurity. Pursuant to the Basic Act on Cybersecurity enacted in November 2014, the National Information Security Center was reorganized and launched as the National Center for Incident Readiness and Cybersecurity (NISC). The primary functions of the center include formulating Japan's cybersecurity policies and collaborating with government ministries and agencies, acting as a liaison in international cooperation, promoting public-private cooperation for protecting critical infrastructures, and collecting the latest cyber threat intelligence. Several other ministries and central government agencies also play a role in Japan's cybersecurity. These are the Ministry of Foreign Affairs (cyber diplomacy), the Ministry of Defense (national security), the National Police Agency (counter-cybercrime), the Ministry of Internal Affairs and Communications (information and communications), the

Ministry of Economy, Trade and Industry (industries in general), and the Digital Agency (digital transformation).

The damages caused by cyberattacks can easily spread across multiple industrial sectors and national borders by impacting supply chains. For this reason, it is crucial to deepen international cooperation in sharing intelligence on cyberattack modus operandi and best practices, and gain support for human resources development. In addition to engaging in bilateral cybersecurity consultations with Australia, Estonia, France, Germany, Israel, India, Ukraine, the United Kingdom, and the United States, Japan is actively engaged in multilateral cooperation with the European Union (EU), the North Atlantic Treaty Organization (NATO), and other organizations.

Since it is indispensable for Japan to ensure a safe and secure business environment in Southeast Asian countries where a large number of Japanese companies operate, Japan has actively promoted cybersecurity cooperation with the Association of Southeast Asian Nations (ASEAN). Beginning in 2009, meetings of the ASEAN-Japan Collaboration on IT Security (currently known as the ASEAN-Japan Cybersecurity Policy Meeting) have been held annually with the attendance of Director-Generals, Deputy Director-Generals, and other senior government officials from those countries to discuss the protection of critical infrastructure. In 2018, the Japanese Ministry of Internal Affairs and Communications established the ASEAN-Japan Cybersecurity Capacity Building Centre in Bangkok, Thailand.

As the host country of the G7 Ise-Shima Summit held in May 2016, Japan issued the "G7 Principles and Actions on Cyber" as one of the outcome documents of the Summit, which included an agreement on G7 cooperation for strengthening cybersecurity. Additionally, the Quad framework between Japan, the United States, Australia, and India also pursues cybersecurity cooperation.

Current situation and challenges

The 2020 Tokyo Olympic and Paralympic Games held during the COVID-19 pandemic came to a close in September 2021 with successful cyber defenses. Although the Games faced 450 million cyberattacks, which was twice as many as experienced in the 2012 London Summer Games, these attacks did not result in any disruption to the operations of Tokyo 2020. This constitutes a remarkable accomplishment in the history of protecting the Olympic Games from cyberattacks. Assistant Professor Brian Gant of Maryville University in the United States, who specializes in cybersecurity, has praised the Tokyo Olympics as a real success story to be emulated by organizers of all types of events.

In response to supply chain challenges during the pandemic, Japan enacted the

Economic Security Promotion Act in May 2022. The legislation aims to ensure the stable supply of critical goods and materials, stable access to key infrastructure services, and support for the development of critical advanced technologies, and none of the three objectives can be achieved in the absence of cybersecurity. For this reason, this law is of key importance in strengthening Japan's cybersecurity.

In September 2021, the Japanese government issued a new Cybersecurity Strategy. This document states that in order to heighten its deterrence capabilities against cyberattacks, "Japan reserves, as options, all viable and effective measures, i.e. political, economic, technological, legal, diplomatic, and all other feasible means." The declaration was a precursor of the National Security Strategy released in December 2022 which has drawn special attention to a concept called "active cyber defense." The introduction of active cyber defense will allow the Japanese government, including the Ministry of Defense and the Self-Defense Forces, to take action for "eliminating in advance the possibility of serious cyberattacks that may cause national security concerns to the Government and critical infrastructures and for preventing the spread of damage in case of such attacks, even if they do not amount to armed attack."

This action would be taken even when cyberattacks "do not amount to armed attack" but can cause major damage. The May 2021 ransomware attack on the Colonial Pipeline in the United States demonstrated that even a financially motivated cyberattack against a single company can cause widespread damage through supply chains and ultimately lead to a national security crisis. The ransomware attack on the Port of Nagoya in July 2023 halted cargo loading and unloading for approximately two days and seriously disrupted the operations of the automotive and apparel sectors. That is why it has become more important to implement active cyber defense and to protect critical infrastructures through public-private partnerships.

Conclusion

Russia's military invasion of Ukraine, which began in February 2022, has involved continuous destructive cyberattacks and espionage against Ukraine. With the prolongation of the war, the countries supporting Ukraine, including Japan, must also stay vigilant about cyberattacks that aim at disrupting military and humanitarian assistance to Ukraine.

In today's world, no economy or national security can stand without digital capabilities. For this reason, cybersecurity is the pivotal point for both economic security and national security. Because the damage from cyberattacks can spread across borders through supply chains, which makes it essential to pursue public-private cooperation both

domestically and globally. Now is the time for Japan to work in unison for protecting critical infrastructure and extending the scale of cyber threat intelligence sharing.

Reference material

Brian Gant (2021), "The Tokyo Olympics are a cybersecurity success story," *Security Magazine*, https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story

Microsoft Threat Intelligence (2022), "New 'Prestige' ransomware impacts organizations in Ukraine and Poland," https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

Tonya Riley (2022), "Iranian hackers planned attack on Boston Children's Hospital last summer, FBI director says," *CyberScoop*, https://cyberscoop.com/iran-hospital-wray-fbi-boston-children/

Mihoko MATSUBARA

Mihoko Matsubara is Chief Cybersecurity Strategist, NTT Corporation, Tokyo, being responsible for cybersecurity thought leadership. She served at the Japanese Ministry of Defense before her M.A. at the Johns Hopkins School of Advanced International Studies on Fulbright. Prior to joining NTT, she worked as Vice President and Public Sector Chief Security Officer for Asia-Pacific at Palo Alto Networks. She served on Japanese government's cybersecurity R&D policy committee between 2014 and 2018.

She is Adjunct Fellow at the Pacific Forum, Honolulu, and Associate Fellow for Cyber at the International Institute for Strategic Studies, London. She published a cybersecurity book in Japanese from the Shinchosha Publishing Co., Ltd. in 2019, which won an award by the Okawa Foundation for Information and Telecommunications in JFY 2020.

She also contributed "Japan's 5G Security Strategy and Competition in Emerging Technologies" to the Strategic Japan project (Competition in New Domains) at the Center for Strategic and International Studies' Japan Chair in 2022. Her second book, *Ukraine's Cyber War*, was published from Shinchosha in August 2023, and awarded by the Digital Policy Forum in 2024.