Recent Cyber Situations and the Bill Introducing Active Cyber Defense

Fueled by the geopolitical conflict between Japan and Russia, DDoS attacks linked to diplomatic and security events in Japan are on the rise. In late February, a Russian hacker group launched an attack in retaliation for the Japan-Ukraine Conference for Promotion of Economic Growth and Reconstruction, which took place in Tokyo on February 19, 2024.
Photo: Cabinet Public Affairs Office

Osawa Jun, Senior Fellow at Nakasone Peace Institute (NPI)

Recent cyberattacks in the context of geopolitics

Since around 2022, state-sponsored cyberattacks have become increasingly prevalent. This is partly due to the rogue cyber nations[1] using cyberattacks to achieve their national objectives. Cyberattacks that do not involve large-scale destruction or loss of life do not constitute armed attacks. These attacks can disable an adversary's critical infrastructure without inciting armed conflict. Furthermore, ransomware attacks on critical infrastructure or supply chains make it difficult to distinguish between attacks by criminal groups and those ordered by a state. This makes it possible to damage an enemy

[1] The US. Department of Defense's 2023 Cyber Strategy designates Russia, China, North Korea, and Iran as countries of cyber concern. (US Department of Defense, 2023 Cyber Strategy, September 2023) https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

country while concealing state involvement. In this respect, cyberattacks have become a convenient tool for rogue cyber nations.

Furthermore, information-theft cyberattacks, which take advantage of the technical characteristics of cyberattacks that make it difficult to identify attackers, are becoming more prevalent, stealing policy information, business secrets, and intellectual property from target countries. Campaigns involving information-theft cyberattacks that appear to target Japan's aerospace and semiconductor industries have also been frequently observed. As illustrated in Figure 1, the Japan Aerospace Exploration Agency (JAXA) experienced four cyberattacks between June 2023 and May 2024, with VPN devices used for teleworking being specifically targeted.[2]

Figure 1: Recent Major Cyberattacks

Time	Target	Victims	Damages	Methods		Type
Until November 2024	Advanced Technology	JAXA	Unauthorized Access Personal Information Leak		Network-penetrating cyberattacks	Information theft
July 2023	Critical Infrastructure	Nagoya Port container terminal	Container Management System Outage (Approximately 2 Days)	Ransomware		Functional destruction
June 2024	Information Platform	KADOKAWA (Niconico)	Destruction of Distribution Cloud System Leak of Business Secrets and Personal Information	Ransomware		Functional destruction
December 2024 - January 2025	Critical Infrastructure	Major Financial Institutions JAL NTT	Disruption of website and online banking services	DDoS		Functional disruption
2023 onward	Japan-US Relations Okinawa Issue	Okinawa Issue	Disinformation Surrounding COVID-19 Vaccines Disinformation Surrounding Okinawan Sovereignty	Disinformation		Information manipulation

On January 8, 2025, the National Police Agency issued a warning announcing that the Chinese cyberattack group "MirrorFace" was responsible for 210 cyberattacks against JAXA and other organizations.[3] From 2019 to 2023, the group conducted "cyberattack campaign A," targeting Japanese think tanks, former government officials, and politicians. From 2023 to 2024, they conducted "cyberattack campaign B," targeting the semiconductor, information and communications, and aerospace industries, infiltrating them through VPN devices. From around June 2024, they

[2] Japan Aerospace Exploration Agency "Report on Unauthorized Access at JAXA," July 5, 2024 https://global.jaxa.jp/press/2024/07/20240705-2_e.html

[3] National Police Agency, "Cyberattacks Using MirrorFace," January 8, 2025. https://www.npa.go.jp/bureau/cyber/pdf/20250108_caution.pdf (in Japanese)

conducted "cyberattack campaign C," targeting academia, think tanks, politicians, and the media.

The "MirrorFace" group used the LODEINFO malware in "Cyber Attack Campaign A" and sent targeted emails impersonating the Liberal Democratic Party's (LDP) public relations department to related organizations during the 2022 Upper House election.[4] Additionally, based on the malware's technical characteristics, "MirrorFace" is believed to have ties to the Ministry of State Security (MSS) of the People's Republic of China.[5]

In addition to information-theft cyberattacks, DDoS (Distributed Denial of Service) attacks, a disruptive cyberattack threatening civilian life, have been observed with increasing frequency.[6] As shown in Figure 1, DDoS attacks targeting major financial institutions occurred between December 2024 and early January 2025. These attacks caused disruptions that prevented online banking and app-based financial transactions for several hours. Cyberattacks believed to be DDoS attacks also occurred at Japan Airlines and JR Central, causing access problems, including disruptions to their reservation sites. DDoS attacks were frequently observed throughout 2024. In addition to attacks over the New Year's holiday period, large-scale DDoS attacks occurred in late February, mid-May, mid-July, and mid-October. The attack targets were not limited to financial services but also included transportation infrastructure, political parties, and industry associations.

Fueled by the geopolitical conflict between Japan and Russia, DDoS attacks linked to diplomatic and security events in Japan are on the rise.[7] In late February, a Russian hacker group launched an attack in retaliation for the Japan-Ukraine Conference for Promotion of Economic Growth and Reconstruction, which took place in Tokyo on February 19, 2024. Attacks in mid-July and mid-October of that year were triggered by joint military exercises in Japan. These attacks are believed to have been carried out by Russia as countermeasures in response to joint training exercises held in July with Japan and NATO member states France, Germany, and Spain (20 fighter jets from these countries arrived in Japan and conducted exercises in the northern airspace at Misawa Air Base) and the Japan-US joint exercise "Keen Sword" (live-fire exercises in eastern Hokkaido), which was announced in October.

---

4 ESET Research, Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities
https://www.eset.com/jp/blog/welivesecurity/unmasking-mirrorface/
5 NTT Security Japan, "Cybersecurity Report 2022.12," January 17, 2023.
https://jp.security.ntt/resources/cyber_security_report/CSR_202212.pdf (in Japanese)
6 Osawa Jun, "Financial Services Targeted by Cyberattacks: Changes in the Geopolitical Environment and the Increase in DDoS Attacks," IINA, June 3, 2024.
https://www.spf.org/iina/en/articles/osawa_03.html
7 Osawa Jun, "Cyberattacks and Disinformation Linked to Diplomatic Events: DDoS Attacks During the G7 Summit," IINA, June 3, 2024.
https://www.spf.org/iina/en/articles/osawa_04.html

As geopolitical conflicts such as the war in Ukraine and the US-China dispute over Taiwan intensify, cyberattacks against Japan, seen as repercussions of these conflicts, are increasing as well. Therefore, it is necessary to understand the intentions of the attackers, improve the predictability of who is being targeted and what types of attacks may be expected, and implement effective defensive measures.

Cyberattack methods change

Since the start of the pandemic in late 2019, many countries have declared states of emergency, imposed lockdowns, and implemented teleworking to ensure business continuity. Consequently, companies and public institutions have set up systems to securely connect to their internal networks from outside using VPNs (virtual private networks). However, since around 2023, cyberattacks targeting these VPN devices, known as "network-penetrating" attacks, have been increasing in Japan (see Figure 1). These attacks exploit vulnerabilities in security equipment designed to protect an organization's internal network, essentially providing access to the network through an unlocked back door. The cyberattacks against JAXA mentioned earlier were of this type.

Cyberattacks that penetrate networks target vulnerabilities in IT security equipment installed at the network perimeter. Since such security equipment is used by many organizations, cyberattacks can be launched using the same techniques against organizations using the same IT equipment, making them highly efficient. Additionally, attackers are increasingly automating cyberattacks. When a new vulnerability is discovered, it is known that a cyberattack campaign using the same method will be launched within 24 hours.

Since around spring 2023, it has been revealed in the United States that the attack group "Volt Typhoon," suspected of having links to the Chinese People's Liberation Army, has been exploiting vulnerabilities in VPN devices to launch cyberattacks against critical infrastructure companies and other entities.[8] After discovering that "Volt Typhoon" was hijacking and exploiting SOHO routers used by homes and small businesses in the United States, the US Department of Justice and the FBI, with court authorization, took compulsory measures to access and neutralize the exploited devices from outside the home.[9] These countermeasures, known as active cyber defense (ACD), have been used in the United States since around 2015.

---

[8] Microsoft Threat Intelligence, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," May 24, 2023.
[9] U.S. Department of Justice, "U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure," January 31, 2024.

Toward the realization of the Active Cyber Defense Bill

In December 2022, Japan revised its National Security Strategy, which included a statement calling for the implementation of Active Cyber Defense (ACD). The statement reads, "Japan will introduce active cyber defense 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 an armed attack."[10] Similar to the United States, Japan is developing legislation that aims to enable compulsory measures to neutralize systems by accessing them externally.

On June 7, 2024, an "Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity" was convened, and on August 7, a summary of the discussions to date was announced. This summary outlines the direction and issues for system development in the three aforementioned areas.[11] However, the transition from the Kishida Fumio Cabinet to the Ishiba Shigeru Cabinet in September 2024, as well as the general election scheduled for October 2024, put the fate of the bill enabling ACD in jeopardy. However, backed by the Research Commission on Security, led by the former LDP Policy Research Council Chairman, Itsunori Onodera, and the Headquarters for the Promotion of a Digital Society Policy Research Council, the Expert Panel's recommendations[12] were submitted to Prime Minister Ishiba on November 29, 2024. A bill introducing Active Cyber Defense[13] was submitted to the 2025 ordinary Diet session. The bill amends related bills in three areas: (1) promoting public-private partnerships, (2) use of communications information, and (3) access and neutralization (sanitization) measures. The bill is expected to fundamentally improve Japan's cyber defense capabilities.[14]

---

[10] Cabinet Secretariat, "Regarding the National Security Strategy," December 16, 2022, p. 21. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf

[11] Cabinet Secretariat Cyber Security System Preparation Office, "Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity: Summary of Discussions to Date," August 7, 2024. https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/giron_seiri/giron_seiri.pdf (in Japanese)

[12] Expert Panel on Enhancing Capabilities in the Field of Cybersecurity, "Saiba anzen hosho bunya de no taio noryoku no kojo ni muketa teigen" (Recommendations for Enhancing Cybersecurity Capabilities), November 29, 2024. https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf (in Japanese)

[13] The official names are "Act on the Arrangement of Relevant Acts in Consequence of the Enforcement of the Act for the Prevention of Damage from Unauthorized Acts against Important Electronic Data Processing Systems" (New Act) and "Bill on the Improvement of Related Laws in Accordance with the Enforcement of the Act on the Prevention of Damage from Unauthorized Acts Against Critical Computers." (Arrangement Act)

[14] The Active Cyber Defense Bill was enacted in May 2025, with portions scheduled to be fully operational by 2027. It will be implemented in government, critical infrastructure, and corporate networks.

Translated from "Saikin no Saiba Josei to Saiba Taisho Noryoku Kyoka Hoan ()," NPI Quarterly*,* Volume 16 Number 2*, pp. 2–3. (Courtesy of Nakasone Peace Institute)* [January 2026]

OSAWA Jun

Senior Fellow at Nakasone Peace Institute (NPI)

Born in 1971. Graduated from the Faculty of Law at Keio University in 1994 and completed the Master's Program at the Graduate School of Law at the same university in 1996 (LL.M.). Served as an analyst, intelligence and analysis service of the Ministry of Foreign Affairs, a foreign policy researcher at the Ministry's Foreign Policy Bureau, a visiting fellow at the Brookings Institution, a visiting fellow at the National Graduate Institute for Policy Studies (GRIPS), and a senior fellow at the Cabinet Secretariat's National Security Secretariat. He assumed his current position in 2025. His specialties are international politics (strategic assessment, cybersecurity). His publications include *Direction of Japan's New Cybersecurity Policy*, Asia-Pacific Review, Vol. 30, No. 3 (March 2024), and co-authored books such as *SNS-jidai no Senryakuheiki: Inboron* (Strategic weapons in the age of social media: Conspiracy theories) (Wedge, 2025), *Shin-ryoiki Anzenhosho: Saiba, Uchu, Mujin-heiki wo Meguru Hoteki-kada*i (New territorial security: Legal issues surrounding cyber, space, and unmanned weapons) (Wedge, 2024), and *Ukuranina Senso wa Naze Owaranainoka: Dejitaru Jidai no Soryokusen* (Why the Ukraine war won't end: Total war in the digital age) (Bunshun Shinsho, 2023).