

CYBER
THREAT
ANALYSIS

Recorded Future®

Insikt Group®

October 8, 2026

内閣府

サイバーセキュリ

— 主権的なサイバー

第1条 (目的)

脅威の検知

通信の分析
不審な接続

IP ADDRESS

203.0.113.24

198.51.100.17

192.0.2.56

Japan Adopts Proactive Cyber Defense Strategy

Japan's Active Cyber Defense Law is driven primarily by state-sponsored or state-aligned cyber threats from China, Russia, and North Korea.

Japan's Active Cyber Defense framework sets new mandatory reporting requirements, structures preventive communications analysis, and allows for limited disruption of attack infrastructure.

Even organizations that have no reporting requirements, such as foreign subsidiaries, non-designated suppliers, individuals, and consumer platforms, become prime targets for state-sponsored threats.

Executive Summary

Japan's Active Cyber Defense (ACD) framework shifts the country from voluntary information sharing and post-incident investigation to mandatory reporting, preventive communications analysis, and limited disruption of attack infrastructure. Beginning October 1, 2026, designated critical infrastructure operators must notify the government about covered systems and report qualifying incidents; those with existing systems have six months to submit initial notifications. New authorities that allow the government to collect and act on communications information (通信情報) will not take effect until November 23, 2027.¹

The transition comes amid persistent Chinese strategic collection, North Korean revenue-driven cyber operations, and Russian cyber espionage. In cases directly linked to Japan, indicators related to these threat activities were frequently observed among victims, overseas affiliates, vendors, carriers, hosting providers, and government agencies. We assess with moderate confidence that connecting those indicators quickly enough to identify broader campaigns, warn potentially affected organizations, and coordinate defensive action will be ACD's principal operational constraint. Its practical reach will extend beyond designated operators: overseas compromises may trigger Japanese reporting duties when they reach covered systems; vendors should expect remediation requests; carriers may be required to assist government measures; and hosting providers may encounter action against malicious systems operating on their infrastructure.

We further assess that improved visibility within covered organizations will likely make foreign subsidiaries, non-designated suppliers, employees, and external platforms comparatively attractive access paths for threat actors without reducing overall attack volume (because initial activity along these routes likely falls outside ACD's mandatory-reporting perimeter or precedes recognition of a qualifying incident). Companies should therefore treat ACD not as a narrow compliance requirement, but as a change to incident escalation, contracting, evidence preservation, and public-private intelligence sharing across their operations and supply chains.

Key Findings

- Japan's Active Cyber Defense is a two-statute framework — Acts 42 and 43 of 2025 — organized around four principal pillars: public-private collaboration, government use of communications information, access and neutralization of cyber threats, and institutional restructuring and independent oversight. Act 42 establishes the reporting, information-sharing, communications-analysis, and oversight framework, while Act 43 amends existing laws to authorize neutralization measures and reorganize Japan's cybersecurity institutions.
- Japan's mandatory cyber incident reporting begins October 1, 2026, but the government's communications-information collection capacity will not enter force until November 23, 2027 —

¹ The Japanese government uses the following kanji 通信情報 in the ACD text, which translates to "communications information." Absent an official Japanese government English translation, we will use that terminology. It may also be referred to as "network traffic" or "telecommunications data" in English.

a gap of roughly 13 months between the reporting duty and the detection capability intended to support it.

- Japanese agencies recorded an eleven-fold increase in cyberattack-related packets from 63.2 billion in 2015 to 686.2 billion in 2024, while 99.4% of observed attack packets used overseas source IP addresses. This is equivalent to roughly one attempted attack per IP address every thirteen seconds.
- Chinese, Russian, and North Korean cyber operations targeting Japan reflect distinct primary drivers: China pursues enduring strategic intelligence collection, North Korea prioritizes sanctions-driven revenue generation, and Russia combines standing espionage requirements with disruption that can track Japanese policy decisions.
- Threat actors will likely emphasize five access paths likely to maintain limited visibility under ACD after reporting begins on October 1, 2026: foreign subsidiaries, non-designated suppliers, individual employees, consumer platforms, and short-lived infrastructure distributed across hosting providers. Organizations occupying these positions may consequently face greater targeting despite having no direct ACD reporting obligation.

Table of Contents

Background	4
The Four Pillars	5
Pillar 1 — Public-Private Collaboration (官民連携)	5
Pillar 2 — Government Use of Communications Information (通信情報の利用)	5
Pillar 3 — Government Access and Neutralization Measures (アクセス・無害化措置)	6
Pillar 4 — Institutional Restructuring and Independent Oversight (組織・体制整備・独立監督)	7
Key Limits on ACD Authority	8
Tokyo's Rationale For the ACD	8
Drivers and Changing Technical Capabilities	11
China	11
China-Linked Cyber Operations against Japanese Entities	12
Russia	13
Russia-Linked Cyber Operations against Japanese Entities	15
North Korea	16
North Korea-Linked Cyber Operations against Japanese Entities	17
Japan-Hosted C2 Infrastructure	18
The ACD's Effectiveness Will Depend on Public-Private Intelligence Integration	19
Outlook	21

Background

Japan's Active Cyber Defense framework (能動的サイバー防御, "ACD") is a package of legal and institutional reforms intended to prevent serious cyberattacks against government and critical infrastructure.² The ACD establishes mechanisms for public-private collaboration (官民連携), government use of specified communications information (通信情報の利用), and narrowly defined authority to access and neutralize systems being used to conduct cyberattacks (アクセス・無害化措置) before they cause significant harm or damage. The framework also restructures the government's central cybersecurity institutions and establishes independent oversight of the framework's most sensitive authorities.

The framework is principally established through two statutes passed by the National Diet (国会) on May 16, 2025, and promulgated on May 23, 2025:

1. **Cyber Response Capability Strengthening Act (サイバー対処能力強化法), Act No. 42 of 2025**
Full statutory title: *Act on the Prevention of Damage from Unauthorized Acts against Important Computers* (重要電子計算機に対する不正な行為による被害の防止に関する法律).

This statute establishes the critical-infrastructure reporting, communications information use, public-private information-sharing, and independent oversight framework.

2. **Cyber Response Capability Strengthening Act Arrangement Act (サイバー対処能力強化法整備法), Act No. 43 of 2025**

Full statutory title: *Act on the Arrangement of Related Laws Accompanying Enforcement of the Act on the Prevention of Damage from Unauthorized Acts against Important Computers* (重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律).

This companion statute amends existing legislation, including the Police Duties Execution Act (警察官職務執行法), Self-Defense Forces Act (自衛隊法), and the 2014 Basic Act on Cybersecurity (サイバーセキュリティ基本法). These amendments authorize access-and-neutralization measures, restructure the government's cybersecurity institutions, and strengthen interagency coordination.

Implementation is phased; the reorganization of the government's central cybersecurity institutions took effect on July 1, 2025, and the independent Japan Active Cyber Defense Oversight Commission (サイバー通信情報監理委員会) was established on April 1, 2026. The public-private reporting and access-and-neutralization provisions will take effect on October 1, 2026. Supplementary Article 1(4) of Act No. 42 [requires](#) the communications-information use provisions to enter force within two years and six months of promulgation, by November 23, 2027.

² As of September 11, 2026, there is no official English translation for the ACD. As a result, all Japanese text was machine-translated for this report.

The Four Pillars

For explanatory purposes, this overview organizes the ACD framework into four principal pillars:

1. Public-Private Collaboration (官民連携)
2. Government Use of Communications Information (通信情報の利用)
3. Government Access and Neutralization Measures (アクセス・無害化措置)
4. Institutional Restructuring and Independent Oversight (組織・体制整備・独立監督)

Together, the pillars summarize the framework's principal government authorities, institutional changes, oversight mechanisms, and legal obligations for public- and private-sector organizations. They reflect a fundamental shift in Japan's cybersecurity posture toward earlier detection, structured public-private cooperation, and preventive disruption, while placing the framework's most sensitive authorities under specialized independent oversight. They do not encompass every provision within the two statutes.

Pillar 1 — Public-Private Collaboration (官民連携)

Pillar 1 creates mandatory reporting requirements and a consent-based information-sharing framework. For ACD reporting purposes, “designated operators” (特別社会基盤事業者) are critical-infrastructure operators designated under the Economic Security Promotion Act that use covered systems — Specified Important Computers (特定重要電子計算機). These include qualifying operators in sectors such as electricity, telecommunications, transport, and finance. Designated critical-infrastructure operators must notify the responsible government minister when they introduce covered systems — Specified Important Computers — and report qualifying cyber incidents (特定侵害事象等) to that minister and the prime minister. The prime minister will establish a statutory council (協議会) for information sharing and countermeasures to prevent damage to Important Computers (重要電子計算機) — the law's broader category of protected computer systems, including Specified Important Computers — from specified unauthorized acts. This statutory council will replace and strengthen the existing 2019 Cybersecurity Council (サイバーセキュリティ協議会). Council members may be required to provide relevant materials and must comply with statutory confidentiality requirements.

In practice, two things change under Pillar 1. First, ACD-specific reporting becomes a statutory duty for designated critical-infrastructure operators that use covered systems — including operators in sectors such as electricity, telecommunications, transport, and finance — thereby reducing the government's dependence on voluntary disclosure once a qualifying incident is detected. Second, government-to-industry sharing enters a protected statutory framework designed to support the distribution of sensitive threat and mitigation information. Pillar 1, therefore, aims to give the government broader visibility into threats while providing participating organizations with actionable warnings. Joining the council is voluntary, but participating members must comply with statutory information-handling and confidentiality obligations and may be required to provide relevant materials.

Pillar 2 — Government Use of Communications Information (通信情報の利用)

Pillar 2 authorizes the government to obtain and analyze specified communications information through two principal pathways:

- Voluntary agreements with participating organizations (当事者協定)
- Defined government measures involving certain foreign-related communications (国外関係通信)

The latter includes foreign-to-foreign communications transiting Japan, as well as limited foreign-to-domestic or domestic-to-foreign communications associated with specified cyber threats. Before a government employee may review acquired data, automated selection (自動選別) must retain only defined mechanical information (機械的情報), such as IP addresses, timestamps, and command information, and delete the remainder. Government measures not based on consent generally require prior approval from the Japan Active Cyber Defense Oversight Commission.

In practice, two things change under Pillar 2. First, the government gains a standing statutory framework for obtaining and analyzing communications information for preventive cyber defense: Japan's pre-ACD Communications Interception Act [authorized](#) interception only for criminal investigations of specified offenses and pursuant to a judge-issued warrant, and Japan lacked a comparable framework for systematic preventive collection and analysis. Second, the limit on what may be retained is enforced by the collection architecture rather than by rules governing analyst conduct. Officials set the selection criteria, but no person may examine the acquired data before the selection is complete, and unselected material must be deleted immediately.

Pillar 3 — Government Access and Neutralization Measures (アクセス・無害化措置)

Pillar 3 establishes access-and-neutralization authority through amendments to the [Police Duties Execution Act and Self-Defense Forces Act](#). Specially designated Cyber Harm Prevention Measure Enforcement Officers (サイバー危害防止措置執行官) may order an administrator to take necessary measures against a computer associated with communications or electronic records identified as being used in malicious cyber activity, or may take those measures directly. Depending on the circumstances, those measures could include:

- Stopping or removing attack software
- Disrupting malicious command-and-control communications
- Changing system settings to prevent an attacker from continuing to control compromised infrastructure

The authority applies when an urgent need exists to prevent serious harm to life, physical safety, or property. Measures generally require prior approval from the Japan Active Cyber Defense Oversight Commission. When circumstances leave no time for advance approval, a measure may proceed, but the Commission must be notified promptly afterward and confirm whether the measure was appropriate.

In practice, Pillar 3 gives designated officers legal authority to intervene against attack infrastructure — including through actions that could otherwise constitute unauthorized access under the 1999 [Act on](#)

[Prohibition of Unauthorized Computer Access](#) — rather than relying on criminal investigation or voluntary remediation. The authority can reach infrastructure outside Japan, but overseas operations are subject to additional restrictions. Police measures against systems not reasonably believed to be in Japan may be conducted only by officers of the National Police Agency (NPA) following consultation with the minister for foreign affairs. In cases involving highly organized and planned threats by a person outside Japan, the prime minister may order the Japan Self-Defense Forces (JSDF) to conduct Communications Protection Measures (通信防護措置) jointly with police, but only when the JSDF's specialized technology or information is indispensable, and the National Public Safety Commission has requested or consented to JSDF involvement.

Pillar 4 — Institutional Restructuring and Independent Oversight (組織・体制整備・独立監督)

Pillar 4 restructures the government's cybersecurity institutions and creates an independent body to oversee the authorities established in Pillars 2 and 3. The reforms include:

- The National Cybersecurity Office (国家サイバー統括室, NCO) replaces the former National Center of Incident Readiness and Strategy for Cybersecurity (内閣サイバーセキュリティセンター, NISC).
- A new cabinet cyber officer (内閣サイバー官) leads the NCO and coordinates cybersecurity policy across the government.
- The restructured Cybersecurity Strategy Headquarters (サイバーセキュリティ戦略本部) is headed by the prime minister (内閣総理大臣) rather than the chief cabinet secretary, with all other ministers of state as members.
- The Japan Active Cyber Defense Oversight Commission (サイバー通信情報監理委員会) grants prior approvals, conducts ongoing inspections, reviews emergency measures taken without advance approval, and may issue recommendations.

In practice, two things change under Pillar 4. First, central coordination is elevated: the Strategy Headquarters is now chaired by the prime minister rather than the chief cabinet secretary, while the cabinet cyber officer and NCO support government-wide coordination. Second, the sensitive authorities in Pillars 2 and 3 are reviewed by a commission separate from the agencies implementing them. Rather than requiring judicial warrants, the framework uses independent administrative review: the Japan Active Cyber Defense Oversight Commission approves nonconsensual communications acquisition and ordinarily approves neutralization measures, conducts continuing inspections, and receives notification of emergency measures. It may issue recommendations and must report annually to the National Diet through the prime minister and publish a summary. Pillar 4 does not establish a separate offensive cyber authority; cross-border neutralization remains governed by Pillar 3.

Key Limits on ACD Authority

The ACD framework expands Japan's preventive cybersecurity authorities but does not provide an unrestricted mandate for surveillance or offensive cyber operations. Its principal statutory boundaries include:

- Communications analysis is not general content surveillance. Human review is limited to automatically selected mechanical information, including technical data such as IP addresses, timestamps, and computer commands, meeting statutory criteria. Purely domestic communications are not a category that the government may target without the parties' consent. If included in data provided under a Party Agreement (当事者協定), they must be excluded through automated selection and deleted without human review.³ Separate laws continue to govern warrant-based interception for criminal investigations.
- Access and neutralization authority is tied to specific mission objectives outlined in the ACD, rather than blanket provisions for government operators. Measures must address communications or electronic records used or reasonably suspected of being used in malicious activity and must be urgently necessary to prevent serious harm to life, physical safety, or property. Overseas measures carry additional procedural and international-law requirements.
- The JSDF cannot independently initiate Communications Protection Measures. Its involvement is limited to highly organized and planned threats by a person outside Japan that present a high risk of serious, difficult-to-recover disruption, and requires a case-by-case finding that the JSDF's technology or information is essential in preventing that disruption. Qualifying action requires a prime ministerial order, a request from or the consent of the National Public Safety Commission, and joint implementation with the police.
- Reporting obligations are not universal. They apply to designated critical-infrastructure operators and covered systems, not to every Japanese organization or local government. Local governments instead fall under the separate [Local Autonomy Act](#), which has required them, since April 1, 2026, to establish cybersecurity policies and implement corresponding measures. Qualifying local-government systems may still receive protection under the ACD framework.

Tokyo's Rationale For the ACD

The ACD framework originates in Japan's 2022 National Security Strategy (NSS), which identified a rapidly deteriorating cyber threat environment and concluded that Japan's legal authorities and institutional capabilities required expansion. The NSS [stated](#) that the "threat of cyberattacks, in which the risk of exposure is relatively low and attackers have an advantage, is growing rapidly." In essence, cyberattacks were seen as low-risk (for the attackers), potentially high-impact means of disrupting operations, stealing information, or advancing strategic and financial objectives while complicating detection, attribution, and timely government response. The NSS [set](#) the objective that Japan's cybersecurity response capabilities should be "strengthened equal to or surpassing the level of leading Western countries." Tokyo's rationale can be organized around three overlapping pressures: a sharp

³ Party Agreement is a consent-based agreement to share specified communications information with the government for cybersecurity analysis. "Party" refers to a participant in those communications, such as a company sending or receiving data.

increase in malicious cyber activity observed by Japanese authorities; several high-profile cyberattacks that disrupted Japanese public- and private-sector operations; and gaps in the government's legal authorities and institutional capabilities for sharing information, analyzing threats, and taking preventive action.

First, Japanese authorities have identified an increase in foreign-origin cyberattacks against Japanese public- and private-sector entities. A September 2025 Japanese NCO briefing [document](#) reported, citing the NPA, that 99.4% of observed attack packets in 2024 originated from overseas IP addresses (**Figure 1**). The same document, citing the National Institute of Information and Communications Technology (NICT), reported an approximately elevenfold increase in cyberattack-related communications between 2015 and 2024, from 63.2 billion observed packets in 2015 to 686.2 billion in 2024. The briefing described this volume as equivalent to approximately one attempted attack per IP address every thirteen seconds, although the underlying measurement represents packets received by sensors rather than confirmed, discrete attacks. Neither dataset identifies actors or intent, and the same briefing explains why the overseas share does not establish that the actors themselves are specifically based overseas: attacks are routed through chains of compromised intermediary machines, so tracing even a domestic-looking source usually leads to an overseas relay. Nevertheless, these figures indicate sustained growth in hostile traffic reaching the Japanese address space.

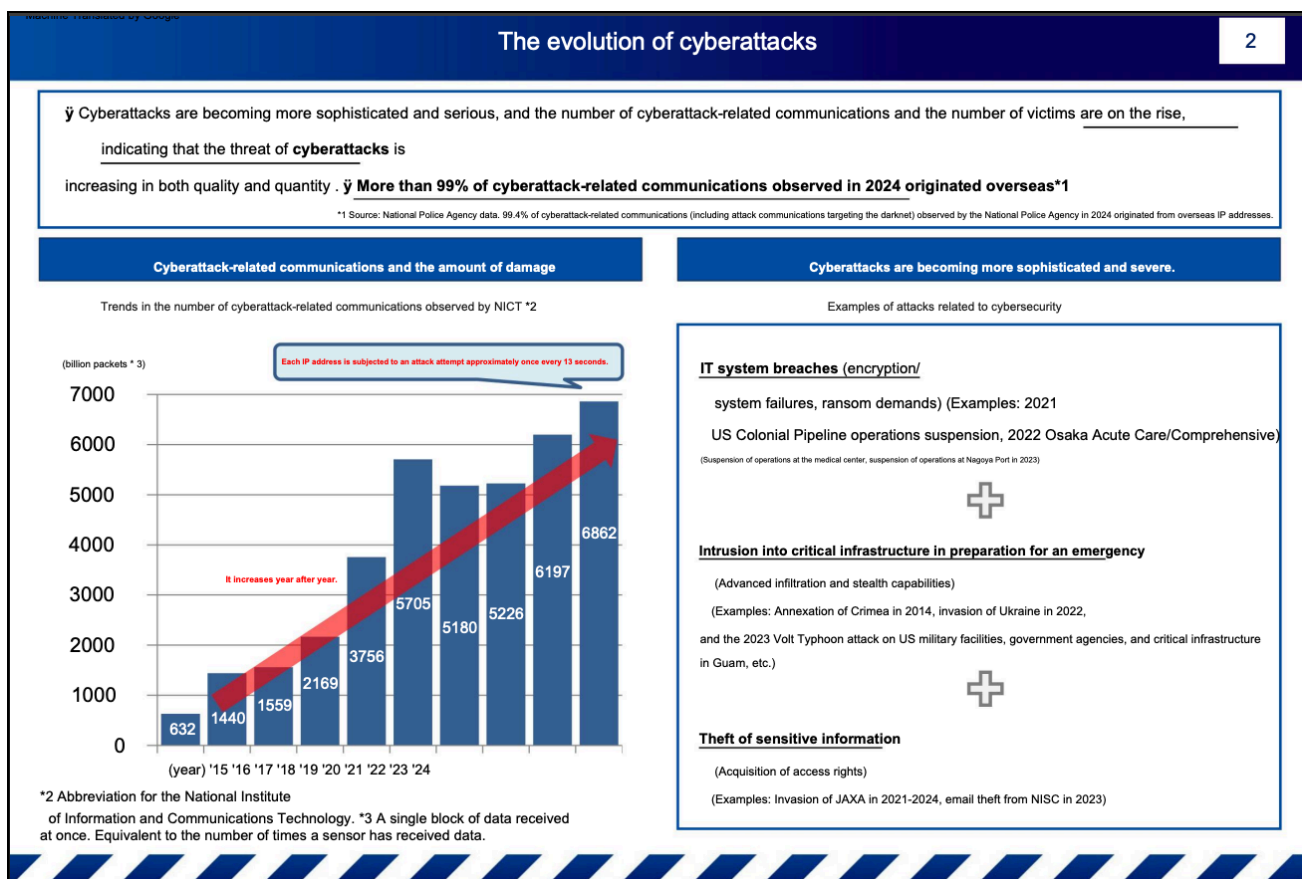


Figure 1: Reported cyberattack frequency against Japan (machine-translated)
(Source: [Japanese National Cybersecurity Office](#))

Second, Japanese authorities assess that these cyber operations represent significant risks to government functions, essential services, and private-sector activity, even when the attackers face a relatively low risk of exposure. Between 2021 and 2024, multiple high-profile cyberattacks targeted Japanese public and private entities, including healthcare, transportation, research, and government organizations. The incidents [included](#) the 2022 Osaka hospital ransomware [attack](#), the 2023 Nagoya Port ransomware [attack](#), sustained intrusions into the Japan Aerospace Exploration Agency (JAXA) [spanning](#) 2021–2024, and the 2022 [exfiltration](#) of email data from the National Center of Incident Readiness and Strategy for Cybersecurity (NISC). Government materials cite these incidents as evidence of cyber threats that have already caused concrete operational disruptions and compromised sensitive information.

Third, Japanese authorities [assess](#) that Japan's existing cybersecurity framework lacked several specific authorities and mandatory mechanisms already adopted by leading Western countries. Measured against the parity objective set in the NSS, the government's comparison, which it describes as non-exhaustive, identifies three gaps: mandatory incident reporting and structured public-private coordination; statutory acquisition and analysis of specified communications information; and authority to access and neutralize infrastructure used in cyberattacks.

- On mandatory reporting and public-private coordination, the United States (US) [enacted](#) the Cyber Incident Reporting for Critical Infrastructure Act in 2022, the United Kingdom (UK) [enacted](#) the Network and Information Systems Regulations in 2018, and Australia [enacted](#) the Security of Critical Infrastructure Act in 2018. In comparison, Japan lacked an equivalent ACD-specific mandatory-reporting mechanism, as the Cybersecurity Council, [established](#) under the 2014 Basic Act on Cybersecurity, remained voluntary.
- On the use of communications information, the government's comparator frameworks include the UK's 2016 Investigatory Powers Act, Germany's [revision](#) of the 2021 Federal Intelligence Service (Bundesnachrichtendienst, BND) Act, the US Foreign Intelligence Surveillance Act 2008 [amendment](#), and Australia's Telecommunications (Interception and Access) Act [amended](#) in 2021. The ACD explanatory [briefing](#) notes that each of these countries places government use of communications information under the oversight of a dedicated, independent body. Japan lacked a comparable statutory framework for acquiring and analyzing specified foreign-related communications information for cyber-defense purposes.
- On disrupting attacker infrastructure, the US [conducted](#) a court-authorized takedown of the Volt Typhoon botnet in 2024, and Canada's Communications Security Establishment (CSE) Act of 2019 [established](#) authorities for foreign cyber operations, allowing the CSE to [neutralize](#) attacker servers abroad. In contrast, Japan lacked a comparable standing authority to access and neutralize attacker infrastructure preventively, particularly before a cyber threat could be addressed through an ordinary criminal investigation.

Taken together, these comparisons reinforced Tokyo's assessment that Japan needed mandatory incident reporting, stronger public-private coordination, a statutory framework for using

communications information, and narrowly defined authority to disrupt attackers' infrastructure. Acts 42 and 43 were enacted to address these perceived gaps.

Drivers and Changing Technical Capabilities

Japan's ACD framework marks a shift toward preventative cyber defense in a changing security environment where cyber operations have become a routine instrument of geopolitical competition and grey-zone warfare below the threshold of armed conflict. Japan's 2025 Cybersecurity Strategy [identifies](#) China, Russia, and North Korea as state-level cyber concerns with implications for Japanese government institutions, critical infrastructure, and strategic industries. The following subsections examine the geopolitical drivers, operational objectives, targets, and technical capabilities associated with each country.

Strained political relations shape the targeting and tempo of Chinese, North Korean, and Russian cyber operations against Japanese entities, but they do not by themselves explain the activity. The three actors are driven by different objectives: Chinese collection likely follows enduring intelligence requirements; North Korean operations likely serve regime revenue-generation priorities; and Russian activity is likely split between standing collection requirements and disruption that responds more directly to Japanese policy.

China

China poses a consequential long-term strategic challenge for Japan, combining persistent gray-zone pressure around the Japan-administered Senkaku Islands with rapidly expanding military capabilities and increasing military pressure on Taiwan. Despite continued diplomatic engagement and extensive economic ties, Japan-China relations [remain](#) constrained by territorial disputes, Chinese military activity [around](#) Japan, and [tensions](#) across the Taiwan Strait.

Beijing likely [uses](#) cyber operations as an instrument of state power to collect political and security intelligence, acquire advanced technology, and gain persistent access to foreign networks. Japan's "Defense of Japan 2025" report [assesses](#) that China is rapidly developing cyber capabilities intended to disrupt adversary communications and reports that China routinely conducts technology theft and surveillance of overseas adversaries in cyberspace. Insikt Group assesses with moderate confidence that sustained regional competition likely creates enduring Chinese intelligence requirements concerning Japanese policymaking, defense planning, alliance coordination, and advanced technology. The China-linked activity described below is consistent with those requirements, although the public evidence does not establish that any individual intrusion was triggered by a specific geopolitical dispute.

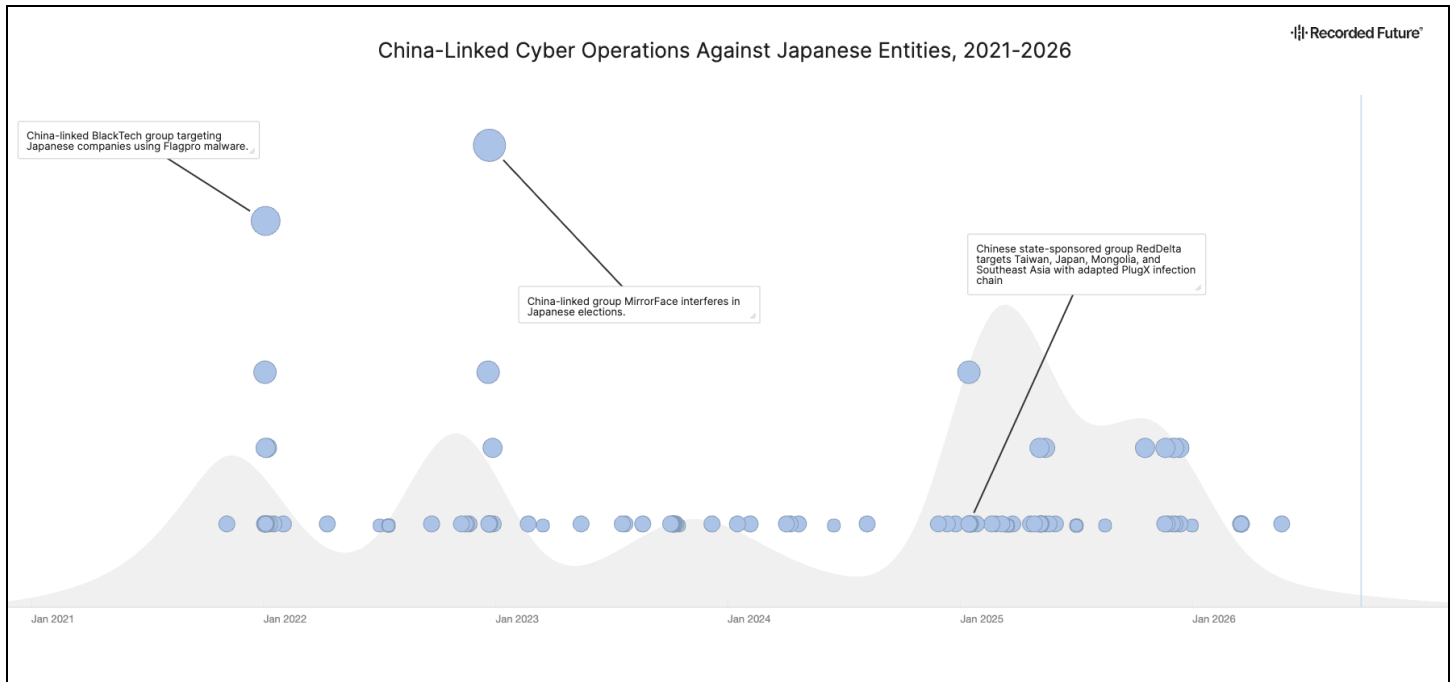


Figure 2: China-linked cyber operations against Japanese entities from 2021 to 2026, identified by Insikt Group
(Source: Recorded Future)

China-Linked Cyber Operations against Japanese Entities

MirrorFace's multi-year campaign against Japanese government and technology targets shows how ACD's reporting and information-sharing mechanisms could help authorities connect intrusions that victims might otherwise view in isolation. Japan's January 2025 MirrorFace (Earth Kasha) [alert](#) assessed that MirrorFace had conducted campaigns with suspected Chinese involvement since approximately 2019 to steal information on national security and advanced technology. The threat actor used phishing and exploited VPN appliances and external servers across government, political, media, academic, manufacturing, telecommunications, semiconductor, and aerospace targets. Across the observed intrusions, MirrorFace compromised Active Directory and accessed Microsoft 365 and virtualization servers, with some activity persisting into 2024. That the campaign ran from approximately 2019 into 2024 before public identification illustrates the reporting latency that the framework is designed to reduce.

BlackTech (Tag-51)'s exploitation of internet-facing devices and trusted cross-border connections shows how ACD's vulnerability coordination and information sharing could expose activity spanning multiple organizations. Around May 2022, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) [confirmed](#) attacks exploiting CVE-2022-1388 on F5 BIG-IP devices at Japanese organizations; the affected organizations confirmed that data stored on the devices had been compromised. JPCERT/CC assessed the activity as related to BlackTech after finding multiple domestic targets and BlackTech-associated malware on an attacker-controlled server. A 2023 joint [advisory](#) from the NPA, NISC, US National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cybersecurity and Infrastructure Security Agency (CISA) separately described BlackTech as PRC-linked

and reported that the actor compromised branch routers at overseas subsidiaries of Japanese and US companies, then abused trusted connections to reach headquarters networks. The advisory did not identify a victim or connect that cross-border technique to the 2022 BIG-IP cases. The initial access occurred at overseas subsidiaries, outside the networks and reporting obligations of the Japanese parent companies, which is precisely the distribution of indicators that the framework's vulnerability coordination and information-sharing mechanisms are directed at.

Recorded Future's RedNovember and RedDelta findings illustrate how ACD's telecommunications analysis and public-private information sharing could provide early warning before the affected Japanese entity or outcome is known. From June 3 through 6, 2024, Insikt Group [observed](#) outbound communications from a RedNovember IP address to Check Point VPN gateways associated with at least 60 organizations, primarily in six countries, including Japan. The activity appeared opportunistic; its timing, after the publication of proof-of-concept code for CVE-2024-24919, suggested a possible exploitation attempt, but we could not identify the Japanese organizations. Recorded Future separately [observed](#) unattributable IP addresses in Japan communicating with known RedDelta PlugX servers from September through December 2024 and identified Japan-based Mongolian Buddhist activists and academics among targets of a March 2023 campaign. ACD's communications analysis and public-private information sharing could help connect those indicators with operator and provider records to identify potentially affected systems and determine whether action is needed.

China-linked actors will likely continue strategic collection against Japanese government, policy, and advanced technology targets. This judgment is based on sustained MirrorFace activity, multinational reporting on BlackTech, and commercial observations of China-linked infrastructure involving Japan. These operations reflect enduring intelligence requirements concerning Japanese policymaking, defense planning, alliance coordination, and technology that would likely persist despite improved bilateral relations. While public reporting identifies actors and techniques more clearly than victims or effects, the ACD's reporting, vulnerability coordination, and communications-information analysis will help investigations, as campaign evidence remains distributed across victims, vendors, governments, and commercial telemetry.

Russia

Russia remains a regional geopolitical rival for Japan, despite longstanding economic ties. The two nations did not [formally](#) sign a peace treaty after World War II, and longstanding territorial disputes over the Kuril Islands in Russia, known as the Northern Territories in Japan, continue to strain bilateral political ties. Russian leadership has publicly [stated](#) that Japan must renounce its claims to the islands for peace negotiations to begin in earnest. This stance was reinforced by Putin's August 13, 2026 [visit](#) to the islands and subsequent statements by former Russian President Dmitry Medvedev that the islands "were, are, and will remain Russian land."

Despite this dispute, Japan and Russia maintain energy ties, including Japanese [investment](#) in the Sakhalin-2 natural gas project. Tokyo has taken steps to maintain access to Sakhalin-2 gas exports, despite [sanctioning](#) Russia following the Russian full-scale invasion of Ukraine. Japan [imported](#) approximately 65 million tons of liquified natural gas (LNG) in 2025, with [approximately](#) 6 million tons, or

9% of its 2025 LNG imports, from Sakhalin-2 alone. Japanese officials [note](#) that the Russian military is maintaining deployment in the Russian Far East near Japan, and is regularly upgrading its military equipment in the region. Japanese [sanctions](#) against Russia following the full-scale invasion of Ukraine in February 2022 created a plausible policy motive for Russia-linked targeting. Recorded Future's observations of Russia-linked cyber operations against Japan increased beginning in 2023, a pattern consistent with — but not proof of — a sanctions-related response. This demonstrates how geopolitical tensions can drive cyber operations.

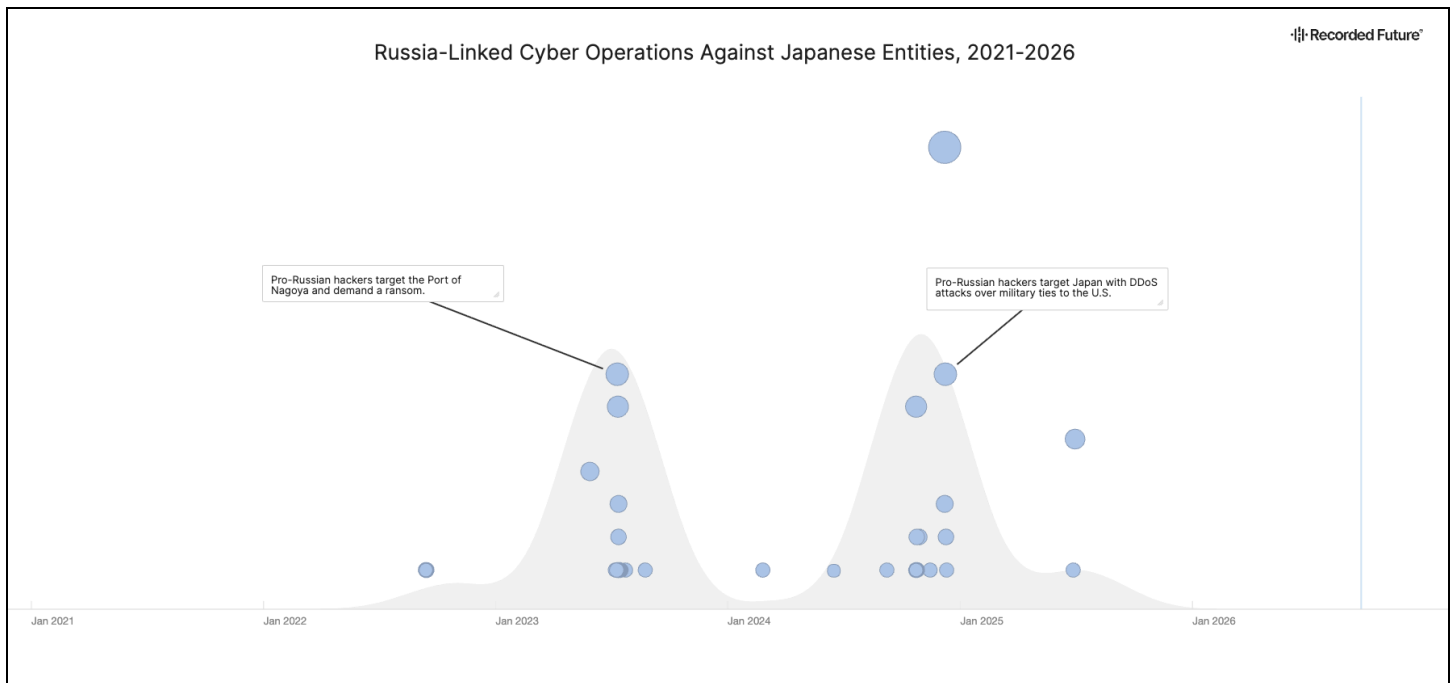


Figure 3: Russia-linked cyber operations against Japanese entities from 2021 to 2026, identified by Insikt Group
(Source: Recorded Future)

Russia-linked cyber activity will likely test ACD's ability to distinguish state-directed espionage from politically responsive disruption by pro-Russia groups. Japan's [2025 Cybersecurity Strategy](#) assesses that Russia [uses](#) cyberattacks to achieve military and political objectives. Covert state espionage likely reflects Russia's standing requirements regarding Japan's alliance coordination, defense posture, and Ukraine-related policy; in at least one case, Japan was [targeted](#) as part of a broader global campaign (see the discussion of BlueBravo, below). Overt disruptive activity, by contrast, has been conducted by nominally independent hacktivist groups whose relationship to the Russian state is contested, though one is the subject of [pending](#) US criminal allegations. The first category (covert state espionage) is likely driven by enduring intelligence collection requirements rather than by particular bilateral disputes, while the second category (overt disruptive activity) is likely driven primarily by Japanese political actions or changes in bilateral relations. This distinction matters under ACD because findings about the actor's location, the degree of organization behind an operation, and the anticipated harm will shape which agency may act and under what authority.

Russia-Linked Cyber Operations against Japanese Entities

Russia-linked cyber threat group BlueBravo's (Midnight Blizzard) targeting of Japanese organizations shows how ACD's public-private information-sharing mechanisms could connect technology-provider warnings with network indicators before an attempted intrusion becomes a confirmed compromise. Beginning on October 22, 2024, Microsoft [observed](#) BlueBravo sending spearphishing emails with attached RDP files to thousands of users at more than 100 organizations. The campaign targeted government agencies, higher education, defense organizations, and NGOs in dozens of countries, including Australia, Europe, the UK, and Japan. The malicious RDP files could map local files, network drives, clipboard contents, peripherals, smart cards, and authentication resources to an actor-controlled server, thereby enabling credential exposure or malware deployment. Microsoft attributes Midnight Blizzard to Russia's Foreign Intelligence Service (SVR), though there is no public confirmation that the SVR or other government body specifically directed the targeting of Japanese institutions. Public reporting has not identified a Japanese organization, quantified the number of Japanese recipients, or established that a Japanese target opened the attachment or was compromised. Although no Japanese compromise has been publicly confirmed, the campaign illustrates how rapidly sharing malicious file and infrastructure indicators could enable ACD participants to take preventive action.

Distributed denial-of-service (DDoS) activity against Japanese government websites in February 2024 shows how ACD's infrastructure-tracking and communications-information analysis could accelerate mitigation, while incomplete attribution of DDoS attacks against Japanese institutions by Russian state-sponsored threat actors would constrain broader conclusions about Russian state direction. Recorded Future [attributed](#) a February 19, 2024, DDoS attack to NoName057(16) and an actor Insikt Group calls the Russian Cyber Army. NPA [reporting](#) separately described February 2024 website-access disruptions believed to have resulted from DDoS attacks and contemporaneous NoName057(16) claims. December 2025 US Justice Department [indictments](#) stated that the Russian government financially backed NoName057(16). The Justice Department characterized NoName057(16) as a state-sanctioned project administered in part by an IT organization created by a Russian presidential order. These are charging allegations, not adjudicated findings, and they do not show that Russian officials selected the February 2024 Japanese targets, ordered the operation, supplied its infrastructure, or coordinated its timing. However, the episode highlights ACD's potential to turn shared incident reports and network traffic data into coordinated mitigation, even when the extent of state involvement remains uncertain.

Russia-linked cyber threat actors will likely continue to target Japanese entities and institutions, driven by geopolitical shifts, bilateral relations, and the goals of state-aligned hacktivist groups. Russian state-aligned cyber intelligence collection will likely persist as part of broader requirements related to Japan's defense posture, alliance coordination, and Ukraine policy, whereas pro-Russia hacktivists will likely concentrate on short-duration disruptions targeting sanctions, aid announcements, and other actions Moscow perceives as hostile. The ACD's value will therefore depend on fusing incident reporting, infrastructure tracking, and communications information quickly enough to distinguish persistent espionage from politically timed disruption and support a proportionate response.

North Korea

North Korea remains one of Japan's most immediate national security concerns. Japan's "Defense of Japan 2025" report [mentions](#) North Korea at least 510 times, and assesses that Pyongyang's military activities pose an "even more grave and imminent threat" to Japan than before, citing its continued nuclear-weapons development, rapidly advancing missile technologies and operational capabilities, and possession of systems capable of striking Japan. Bilateral relations are further constrained by longstanding, [unresolved](#) abductions of Japanese citizens. Together, these military capabilities and unresolved bilateral issues provide the broader national security context in which Tokyo assesses North Korea's cyber activity against Japan.

Pyongyang has [made](#) cyber operations and fraudulent IT-worker employment schemes important instruments of state policy, [using](#) them to steal cryptocurrency, generate foreign currency, evade international sanctions, and acquire sensitive information. It also uses cyber operations to fund its weapons program. In June 2026, the Japan-US-ROK Trilateral Diplomatic Working Group on North Korea's Cyber Threats [stated](#) that North Korean cryptocurrency theft and IT-worker activity (tracked by Insikt Group as PurpleDelta) fund the country's unlawful weapons-of-mass-destruction and ballistic missile programs. We assess that this funding relationship places North Korean cyber activity within the same national security problem set as its nuclear and missile development, rather than treating it as a separable financial crime or sanctions-evasion issue.

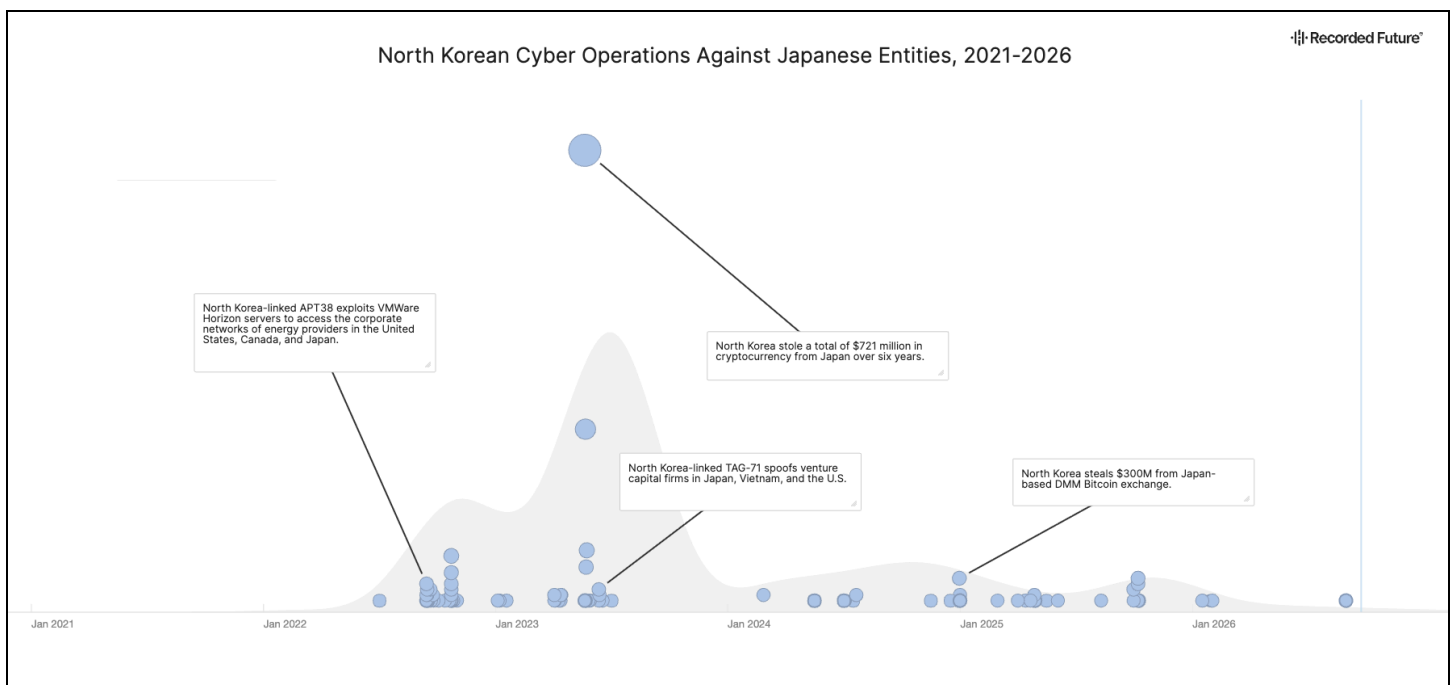


Figure 4: North Korean state-sponsored cyber operations against Japanese entities from 2021 to 2026, identified by Insikt Group (Source: Recorded Future)

North Korea-Linked Cyber Operations against Japanese Entities

Japan [warned](#) of sustained North Korean targeting against its cryptocurrency sector before the largest publicly attributed loss in 2024. In October 2022, Japan's Financial Services Agency, NPA, and NISC warned that attacks similar to those associated with Lazarus Group had been conducted against Japanese cryptocurrency exchanges and assessed that relevant Japanese businesses had been targeted for several years. The agencies identified executive impersonation, phishing emails, false social media accounts, malware delivery, and subsequent network access as characteristic methods used to steal cryptocurrency and assessed that such attacks would continue. Insikt Group's 2023 Crypto Country [report](#) placed the Japanese warning within a broader expansion of North Korean cryptocurrency targeting.⁴ Together, these sources indicate that Japan had identified a sustained threat before specific victims and losses were publicly attributed. The advisory shows that these intrusion methods were already recognized; ACD's reporting and information-sharing mechanisms could help connect those general warnings with evidence of specific attacks and support coordinated defensive action. This is the gap that the ACD's mandatory reporting and structured information-sharing provisions are very likely intended to address.

The May 2024 theft from Japanese cryptocurrency exchange DMM Bitcoin shows how a supplier compromise can cause customer losses, underscoring the need for ACD's reporting and information-sharing mechanisms to connect threat activity across organizations. The NPA, US FBI, and US Department of Defense (DOD) Cyber Crime Center [attributed](#) the theft of 4,502.9 BTC, worth approximately ¥48.2 billion at the time (\$308 million USD in 2024), to North Korean actors tracked as TraderTraitor. An actor reportedly posed as a recruiter, contacted a Ginco employee via LinkedIn, and sent a malicious Python script, disguised as a pre-employment test, through GitHub. The Ginco employee had access to Ginco's wallet-management system and was compromised after copying the code to a personal GitHub page. After compromising the employee, TraderTraitor exploited stolen session-cookie information to impersonate the employee and access Ginco's unencrypted communications system, then likely used that access to manipulate a legitimate DMM Bitcoin transaction request, resulting in the transfer of the stolen assets to wallets they controlled. No single organization held a complete view of the incident. This is the visibility gap that the ACD's communications-information provisions (Pillar 2) are directed at: acquiring and analyzing specified communications information to identify attack infrastructure before compromise, rather than relying on victims to report incidents and details after the fact.

The DMM hack and Kaspersky's observations of BlueNoroff (APT38) campaigns in 2025 demonstrate both the utility and limits of the ACD framework: public-private information sharing and communications-information analysis may help identify malicious infrastructure and downstream command-and-control (C2) activity, but initial social-engineering contacts can occur through third-party platforms before an organization has observable indicators or a reportable incident. In October 2025, Kaspersky [reported](#) on two campaigns — GhostCall and GhostHire — that it attributed to

⁴ Insikt Group stated that Japanese companies had been successfully compromised and had cryptocurrency stolen. However, the cited October 2022 Japanese advisory did not identify a specific victim, confirmed compromise, or loss. This report therefore uses the narrower official characterization to conduct phishing attacks, whereas GhostHire threat actors posed as recruiters and delivered malicious coding tests via.

BlueNoroff with medium-high confidence. Its telemetry detected several GhostCall-infected macOS hosts in Japan and identified individuals in Japan and Australia as GhostHire victims. GhostCall threat actors posed as investors and used fraudulent Zoom or Microsoft Teams meetings to conduct phishing attacks, whereas GhostHire threat actors posed as recruiters and delivered malicious coding tests via Telegram bots, GitHub repositories, or ZIP archives. The campaigns' malware targeted cryptocurrency wallets and a broader range of browser credentials, password vaults, collaboration platforms, cloud services, and DevOps data. Kaspersky reported on the infected devices and individual victims in Japan without disclosing their identities or quantifying Japan-specific financial losses; the evidence, therefore, establishes a compromise but leaves its financial consequences unclear. The GhostCall and GhostHire operations and the DMM hack used trusted third-party platforms to approach individuals and deliver malicious code, illustrating why ACD's early-warning efforts would benefit from information sharing among platform providers, suppliers, and potentially affected organizations.

Beyond these confirmed compromises, Insikt Group's TAG-71 [research](#) shows what precursor activity can look like before a victim or loss is publicly established. Between September 2022 and March 2023, Insikt Group identified 74 domains resolving to five IP addresses and six malicious files in a cluster that spoofed financial and venture-capital organizations in Japan, Vietnam, and the US. The infrastructure supported phishing, malware delivery, and C2 activity, illustrating how ACD's information-sharing mechanisms could help authorities and private organizations connect related indicators, check whether their systems have been targeted, and issue warnings before further harm occurs.

North Korea will almost certainly remain a persistent, financially motivated cyber threat to Japan-based organizations in the near term. This assessment is based on the national security context established above, in which North Korean cyber operations function as state policy rather than opportunistic crime, as well as geopolitical drivers, bilateral relations between Tokyo and Pyongyang, Japan's earlier warning of sustained targeting, and the confirmed DMM Bitcoin thefts. However, the underlying driver is Pyongyang's need to generate foreign currency revenue to offset extensive international sanctions, which shows no indication of diminishing absent significant sanctions relief or a sustained fall in cryptocurrency values. This pattern makes public-private threat-intelligence sharing, malicious-infrastructure tracking, and cross-organizational response coordination operationally relevant to the ACD framework because the first indicator, initial compromise, and ultimate loss may occur at different organizations.

Japan-Hosted C2 Infrastructure

Japan-hosted C2 infrastructure is the clearest target for the ACD's access-and-neutralization authority, though the distribution of infrastructure across commercial providers means identifying the operators behind it may depend on records that ACD does not automatically entitle the government to obtain from every hosting provider. Insikt Group identified 105 distinct IP addresses likely geolocated in Japan and associated with C2 observations in the last five years. The cohort spanned 40 autonomous system numbers and reflected a broad commercial hosting ecosystem rather than a concentration within a single provider. The web hosting providers include a large US hyperscaler, Vultr/The Constant Company, BGPNET, xTom Japan, CTG Server, and Cloudie. That dispersion means the framework's

neutralization authority, though available for domestically hosted infrastructure, must be exercised provider by provider rather than against a single point of concentration.

Provider cooperation is not always a legal prerequisite for neutralization: under the ACD, a designated officer may act directly against a computer or order its administrator to take measures. Commercial hosting providers have mandatory ACD incident-reporting duties only if they qualify as designated operators using covered systems. Providers outside that reporting category may nevertheless host infrastructure subject to lawful neutralization. Identifying the customer behind that infrastructure and preserving relevant records may still require provider assistance. Of the cohort identified by Insikt Group, 77 IP addresses (73.3%) were associated with cloud, VPS, or commercial hosting networks, while the remaining 28 were unresolved rather than confirmed as non-hosting infrastructure. Likely Japanese geolocation does not establish physical location, actor control, or use against Japanese targets. Because relevant records may be rotated or deleted under provider-specific retention schedules, ACD's operational value will depend on tested coordination channels capable of converting infrastructure observations into timely, lawful action.

The ACD's Effectiveness Will Depend on Public-Private Intelligence Integration

The ACD will give Japan more cyber data; its effectiveness will depend on turning that data into shared, actionable intelligence. The government's policy for [implementing](#) the ACD organizes implementation around three functions — collection, integrated analysis, and dissemination — and relies on system notifications, mandatory incident reports, monitoring communications information, and the statutory council for information sharing and countermeasures exchanges. The ACD's principal operational challenge will likely be linking an operator's incident, a supplier's vulnerability, a telecom provider's network indicator, and government intelligence quickly enough to recognize a campaign before its effects spread. Infrastructure tracking and traffic analysis will provide the greatest incremental early-warning value because they can reveal related activity before a victim is identified. Incident reporting and vulnerability coordination will validate those signals, while response coordination becomes decisive after the threat is recognized.

Government integration will require specialization without fragmentation. Under official [implementation materials](#), the Cabinet Office will perform much of the ACD's statutory collection, analysis, and dissemination, while NCO must integrate that work with law-enforcement reporting, defense and foreign-partner intelligence, sector regulators, and national strategy to produce a common analytic picture. The same information must support different government decisions; an indicator adequate for early warning may remain insufficient for police neutralization, JSDF involvement, or diplomatic consultation. The central requirement will therefore be an analytic process that identifies what is known, what is inferred, and what remains missing, while allowing agencies to reach and revise coordinated judgments without obscuring source limitations or statutory boundaries.

Private organizations will become intelligence producers, not merely recipients of government warnings. Under the ACD, [designated](#) operators must submit system notifications and report qualifying incidents — but detection is the harder half, because latent intrusions may remain unrecognized until

shared indicators reveal related activity. Affected telecommunications carriers will need to support lawful traffic acquisition while maintaining data quality, security, and privacy safeguards. Technology vendors will need to help validate and remediate vulnerabilities, while local governments — although outside the mandatory-reporting requirements — will need channels to receive warnings and contribute relevant incident information. Because membership in the statutory council for information sharing and countermeasures is consensual, companies' willingness to join and contribute useful intelligence will likely depend partly on whether the government provides timely, actionable information in return.

Several recurring access paths available to threat actors sit outside the ACD's mandatory reporting perimeter or arise before its duties attach. Academic, media, and think tank targets are not generally designated operators; compromise of an overseas subsidiary may not become reportable until it reaches a covered Japanese system; and a lure delivered through a consumer platform may precede any detectable or qualifying incident. When a non-designated service provider is breached upstream of a designated operator, the provider itself may likewise have no ACD reporting duty. There will likely be persistent reporting gaps around third-party providers, foreign subsidiaries, and individuals because these gaps are not addressed in the formal scope now defined in [Cabinet Order No. 47 of 2026](#) and the accompanying [implementing ministerial order](#). These gaps do not place subsequent malicious activity wholly outside the ACD, but they may delay mandatory reporting and leave early warning dependent on voluntary disclosure or other government collection.

Outlook

Designated operators will assume the ACD's first direct compliance and detection burdens [on](#) October 1, 2026, when mandatory incident reporting begins. Operators with covered systems already installed will have six months to submit their initial system notifications. The government's communications-information authorities, however, will not take effect [until](#) November 23, 2027. Reporting obligations may therefore precede government threat detection and analysis by as much as thirteen months. During that interval — and after the capability becomes operational — companies should treat government warnings as supplementary to, rather than a substitute for, their own monitoring, incident recognition, and escalation processes.

Organizations outside ACD's mandatory reporting requirements should not assume that non-designation reduces their exposure. Threat actors will likely adapt by emphasizing access paths that provide limited visibility under the ACD. These include foreign subsidiaries, non-designated suppliers, individual employees, consumer platforms, and short-lived infrastructure distributed across multiple hosting providers. Organizations occupying those positions, such as service providers upstream of designated operators, overseas affiliates of Japanese parent providers, and firms whose staff are reachable through professional platforms, may therefore face more targeting after October 2026, not less.

Multinational organizations should expect that a compromise beginning in an overseas network may become reportable by their Japanese entity once the Japanese operator recognizes qualifying activity involving a covered domestic system — even if the overseas investigation remains incomplete or outside the Japanese entity's control. Technology vendors should anticipate requests for vulnerability information and remediation support without becoming regulated operators themselves. Telecommunications carriers and hosting providers face more direct operational effects: carriers may be required to assist government measures, while hosting providers may receive remediation orders or, under narrow conditions, encounter government action against malicious systems operating on their infrastructure. These effects will likely influence contracts, incident-response plans, evidence-preservation procedures, and information-sharing arrangements beyond the companies directly subject to ACD reporting duties.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com