JUNE 2025

Norms in New Technological Domains

What's Next for Japan and the United States in Cyberspace

By Koichiro Komiyama

*This report is part of **Strategic Japan**, a CSIS Japan Chair initiative featuring analysis by Japan's leading foreign policy scholars on key regional and global challenges and the implications for the U.S.-Japan alliance.*

Introduction

Cybersecurity and national security have become inseparably intertwined in recent years. Once regarded as a global commons—an open and interconnected frontier—cyberspace has rapidly been reframed both as the fifth domain of warfare (the other four being land, sea, air, and outer space) and as the front line of great power competition. In addition, cyberspace has proven to be far more centralized than many initially believed. It is a space where just eight providers generate 65 percent of all internet traffic. **A triadic competition**—specifically, the contest among democracies, authoritarian states, and big tech companies—constantly arranges (and rearranges) cyberspace.

In February 2025, Japanese Prime Minister Shigeru Ishiba visited Washington, D.C., and held a summit meeting with President Trump. On that occasion, the two leaders issued a **joint statement**, declaring that they "intend to expand bilateral security cooperation in cyberspace by leveraging new technologies such as artificial intelligence and secure and resilient cloud services to deepen information-sharing." The statement positioned cyber as a core pillar of the U.S.-Japan alliance and signaled a willingness to jointly confront emerging digital threats through shared technological and operational capacities. Just as the U.S.-Japan security alliance remains an indispensable mechanism for regional stability, the joint statement clearly reflects both countries' recognition that enhanced bilateral cyber cooperation is essential for ensuring order and stability in an increasingly unstable cyberspace.

This white paper examines how Japan and the United States should pursue bilateral cooperation in cyberspace within the framework of the current U.S.-Japan alliance, which remains one of the most

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

robust security partnerships in the world. To that end, the paper outlines Japan's current cybersecurity threat landscape and key legislative developments. It also identifies three core policy recommendations for strengthening Japan's cyber resilience that can ultimately contribute to the alliance.

Japan's Threat Landscape

Almost daily, Chinese and North Korean threat actors target Japan through a range of cyberattacks. Chinese threat actors systematically conduct near-continuous cyber espionage against Japanese targets, focusing in particular on achieving political and military advantages. Major sectors under attack include shipbuilding, aerospace, manufacturing, and government research. For instance, in January 2025, Japan's National Police Agency (NPA) **reported** that the Chinese MirrorFace group carried out cyberattack campaigns against sectors covering semiconductors, telecommunication providers, manufacturing, aerospace technology, and academia, among others. Moreover, investigators have noted that Chinese hacking waves against Japanese targets tend to mirror Beijing's working hours—including pausing on Beijing's national holidays—indicating state sponsorship. U.S. and Japanese officials have also **warned of Chinese firmware implants in the routers** and telecommunication equipment used to maintain long-term access to government and corporate networks. China's cyber operators represent a near-constant espionage threat to both Japan's strategic industries and to its government. Finally, Chinese cyberattacks are highly sophisticated and often target sensitive information related to national security.

North Korea, in contrast, remains financially motivated, focusing its efforts on stealing cryptocurrency, such as Bitcoin, from Japanese cryptocurrency exchanges. For example, the Lazarus Group has carried out several major cryptocurrency heists against Japanese targets. To cite one attack, in December 2024, Japan's NPA and U.S. agencies jointly **disclosed** that Lazarus-linked hackers—tracked as "TraderTraitor"—stole 4,502.9 bitcoin ($307 million USD) from a Tokyo-based cryptocurrency exchange the prior May, explicitly identifying TraderTraitor as part of the Lazarus Group. Japanese authorities have issued multiple advisories warning domestic cryptocurrency exchanges about North Korean phishing campaigns, which typically involve LinkedIn/social media lures or fake recruiters in efforts to trick exchange employees into executing malware on their work computers. Experts note that cyber theft of various cryptocurrencies is a preferred revenue stream for North Korea, as, in general, cryptocurrency is managed more loosely than fiat currencies. Although North Korean actors also engage in ransomware and intellectual property theft, to date, their most visible activities in Japan have been aimed at draining cryptocurrency.

Japan's Preparedness

Despite Japan's significant economic stature—it is the world's fourth-largest economy by GDP—its cybersecurity posture is widely perceived as increasingly lagging behind its peers. For example, the Harvard Belfer Center's **National Cyber Power Index** (NCPI) ranked Japan ninth in 2020, dropping it to sixteenth in 2022. Similarly, the International Institute for Strategic Studies' (IISS) ***Cyber Power and Future Conflict*** report categorized Japan as a Tier 3 cyber power, placing it alongside North Korea.

One reason for Japan's relatively low evaluations is that its domestic debates and policy efforts are not being effectively communicated to international audiences. In fact, in some cases, international reports appear to rely on outdated information or even miss Japanese-language sources entirely. This is a failure of strategic messaging on Japan's part. Moreover, although analysts praise Japan's international

contributions to the United Nations, the G7, and the G20; its domestic cyber-governance, including prosecution of criminal cyber activity; and its steady capacity-building program for the ASEAN countries, the country's offensive cyber capabilities are seen as lacking. The NCPI and IISS reports both point to Japan's limited cyber-counterstrike capabilities as a major weakness. Both reports incorporate evaluations of offensive cyber capabilities and, in some cases, the "intent" to use such capabilities as part of their evaluation criteria. According to these international analyses, Japan clearly lacks offensive cyber capabilities, and this negatively affects its international standing.

> *Despite Japan's significant economic stature—it is the world's fourth-largest economy by GDP—its cybersecurity posture is widely perceived as increasingly lagging behind its peers.*

Although these assessments may be subject to debate, the reasons behind Japan's lower rankings are clear: Both reports emphasize Japan's limited capability to conduct offensive cyber operations, particularly within the Japan Self-Defense Forces. This is not a new issue. The absence of robust counterstrike capabilities has long been recognized as a critical gap in Japan's national security posture. In an attempt to address this gap, Japan's **second National Security Strategy** (published December 2022) explicitly stated: "In order to ensure secure and stable use of cyberspace, especially the security of the nation and critical infrastructures, the response capabilities in the field of cybersecurity should be strengthened equal to or surpassing the level of leading Western countries." To achieve this goal, Japan has begun enacting and implementing legislative reforms.

Legislative Shift: Japan's Active Cyber Defense Bill

Japan's constitution and legal framework have traditionally constrained offensive cyber measures. Article 9 of the country's constitution renounces war and prohibits Japan from maintaining traditional military forces, which has long been understood to mean that Japan can only take defensive—and not offensive—actions. Furthermore, **critics** have pointed out that preemptive actions might violate both **Japan's Telecommunications Business Law** and its **Act on the Prohibition of Unauthorized Computer Access**. In practice, this has meant that Japan could detect and defend against cyberattacks but had no clear legal mandate to infiltrate adversary networks or neutralize threats before they materialized. In fact, until very recently, Japan's approach to cyber threats was essentially reactive: focusing on hardening networks and coordinating with allies, rather than on "hacking back."

In recent years, however, Japan's cyber policy has shifted toward limited "active defense." The Ishiba administration (building on earlier proposals led by Ishiba's predecessor, Fumio Kishida) has introduced a so-called Active Cyber Defense Bill, complete with amendments to several key laws, including **the Self-Defense Forces Law**, **the Basic Act on Cybersecurity**, and **the Police Duties Execution Law**. The proposed legislation passed the Diet in May 2025, and is scheduled to come into effect no later than November 2027. If enacted as planned, the legislation would bring about several major changes in Japan's approach to cybersecurity.

First, the bill and amendments to existing laws will expand the authority of the National Police Agency and the Self-Defense Forces, empowering them to conduct active cyber measures. As such actions must be carried out in a coordinated manner between the two agencies, a newly established organization within the Cabinet Secretariat will lead the coordination, working closely with the National Security Secretariat (NSS) as well.

Second, Japan will implement a cyber-traffic monitoring mechanism. The government and Internet Service Providers (ISPs) both will be permitted to analyze cross-border data traffic traversing Japan's cyber infrastructure. Public concern over protecting the confidentiality of communications, as guaranteed by Japan's constitution, remains strong in Japan. During deliberations in the House of Representatives, strong reservations were voiced—particularly by opposition parties—regarding potential infringements on privacy. As a result, the bill was amended to explicitly state that the confidentiality of communications—as guaranteed under Article 21—shall not be unduly restricted, keeping any domestic cyber communications off-limits. A new independent oversight body will supervise and authorize these activities.

Third, the bill will strengthen public-private partnerships and establish a new central cybersecurity authority, replacing the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) housed in the Cabinet Office. This marks a substantial institutional shift: The Cybersecurity Strategic Headquarters will be restructured; the prime minister will serve as its chair; and all cabinet ministers will be included as members. The "Cabinet Cybersecurity Officer"—a new position holding vice-ministerial rank—will be created within the Cabinet Secretariat to oversee cybersecurity-related affairs. While not mandatory, the law also provides the legal basis for appointing a Minister of State for Cyber Affairs within the Cabinet Office. The new organization will act as the quarterback for Japan's cybersecurity by leading government efforts and advancing cyber capabilities in coordination with the private sector.

Among security and cybersecurity experts in Japan, there are concerns—particularly regarding communications monitoring—that the law's scope might be too limited to detect threats effectively. It is true that the bill does not provide a complete solution to the goals set out in Japan's 2022 National Security Strategy. The new law and accompanying amendments should be seen as an initial step toward the longer-term strengthening of Japan's cybersecurity capabilities, not the ultimate answer.

Three Policy Priorities for the U.S.-Japan Alliance

U.S.-Japan cooperation in cyberspace has made steady progress over the past decade, evolving from initial information-sharing frameworks to more integrated efforts in defense planning and multilateral norm-building. As explained previously, Japan's Active Cyber Defense Bill marks a turning point for the country: It is expected to further strengthen operational coordination between Japan's Self-Defense Forces and the U.S. military, particularly in responding to state-sponsored cyber threats.

However, cybersecurity challenges cannot be fully addressed through defense cooperation alone. Given the increasing complexity and interconnectedness of digital threats, the next phase of alliance-based collaboration must extend into civilian domains, private-sector infrastructure, and multilateral norm-setting. The following section proposes three concrete areas—outside of the military sphere—where deeper U.S.-Japan cooperation can help shape a more resilient and secure cyberspace.

> *Japan's Active Cyber Defense Bill marks a turning point for the country: It is expected to further strengthen operational coordination between Japan's Self-Defense Forces and the U.S. military, particularly in responding to state-sponsored cyber threats.*

PROTECTING THE PUBLIC CORE OF THE INTERNET

The vulnerability of physical communication infrastructure, such as subsea cables, has emerged as a growing concern. This was brought to the forefront when, in late 2024, undersea cables in the Baltic Sea connecting Sweden-Lithuania and Finland-Germany were deliberately severed, raising concerns about the possibility of **NATO's Article 5 being triggered**. While Article 5 states that an armed attack against one or more NATO members shall be considered an attack against them all, thus obligating collective defense, cyber and hybrid attacks fall into a legal and strategic gray zone. The increasingly visible exposure of physical infrastructure—particularly communications cables vital to military coordination and civilian life—to deliberate sabotage by threat actors has pushed NATO allies to consider whether such actions meet the threshold for a collective response. The 2024 incident in the Baltic Sea was not the exception; the world had already witnessed Russian interference with European satellite communications during the invasion into Ukraine in 2022. Subsequently, in January 2025, a cargo vessel flagged as African but actually **operated by a company affiliated with individuals in China** sabotaged Taiwan's international cable. Protecting communication infrastructure is a critical economic and national security concern for the international community that merits urgent attention, not only to safeguard civilian and commercial connectivity but also to deter malign actors from exploiting physical infrastructure vulnerabilities as instruments of coercion, espionage, or hybrid warfare.

As an island nation, Japan unsurprisingly relies on subsea cables for 99 percent of its international communications. What is less widely known is that Japanese companies possess world-leading technologies in manufacturing fiber-optic cables, repeaters, and related equipment. In addition, Japanese telecom companies operate around seven cable-laying vessels—the largest such fleet in East Asia. In the face of various connectivity crises in that region, Japan is positioned to play a critical leadership role in tackling this challenge.

Even if the physical strength of cables can be increased, or multiple cables are laid to create redundancy, it remains challenging to completely prevent cable cuts. The most effective way to avoid this type of sabotage is to raise the cost of destroying the cables beyond any benefit that would be obtained through their destruction. The threat of physical sabotage—whether in wartime or peacetime—necessitates a normative international approach to protecting what Dennis Broeders of Leiden University called the "**Public Core of the Internet**." Broeders argues that protecting the core of the internet—for example, the Domain Name System (DNS), internet exchanges, and key physical infrastructure including subsea cables—is essential for maintaining the internet's stability, security, and openness. He warns against threats such as state-sponsored cyberattacks, monopolies, and efforts to fragment the internet through national regulations. Instead, Broeders advocates for international cooperation, stronger governance, and various cybersecurity measures to ensure that the internet

remains decentralized and resilient. In short, he calls for efforts to safeguard the internet's core to preserve its global, open nature.

> *Protecting communication infrastructure is a critical economic and national security concern for the international community that merits urgent attention.*

The core-protection endeavor can be split into two different streams of work. First, Japan and the United States should lead efforts to develop peacetime norms prohibiting cyberattacks on this public core, including contributing to ongoing UN processes such as the **Open-ended Working Group** (OEWG). Second, the wisdom of international humanitarian law should guide international actions, particularly in times of armed conflict. The International Committee of the Red Cross (ICRC) is currently exploring how to apply international humanitarian law (IHL) to cyberspace. One group of scholars proposed an idea called "**Digital Emblem**" that would serve as a machine-readable marker embedded in digital systems used by humanitarian organizations, thereby enabling military cyber operators to identify and avoid targeting these systems during armed conflict. For over 150 years, the ICRC has employed the images of a red cross or a red crescent to convey a simple message: Those who wear these symbols, or facilities and objects marked with them, must be protected from harm. The concept of a digital emblem is the same. Digital watermarks or fingerprints could be added to systems used by hospitals and humanitarian actors, indicating to others that such systems should be kept from harm.

HARMONIZING IOT SECURITY ACCREDITATION ACROSS JURISDICTIONS

The European Union has emerged as a global leader in regulating cyberspace. Rules created in Brussels increasingly shape global standards, with the **General Data Protection Regulation** (GDPR) being the most prominent example. In addition, the European Union's **Digital Services Act**, which imposes new responsibilities on large online platforms, has already influenced policy debates in Japan and elsewhere.

Another notable EU initiative is its **Cyber Resilience Act**, which introduces an accreditation and labeling system for Internet of Things (IoT) devices. IoT devices are always connected to the internet and often run with weak passwords or outdated firmware, making them attractive targets for hackers. Recent cyber campaigns, including China's APT group Volt Typhoon, **have exploited vulnerable IoT devices**—specifically SOHO routers—to infiltrate networks while evading detection. To address this vulnerability, the use of insecure IoT products must be reduced and regulated.

The European Union is taking the lead in this field. With its Cyber Resilience Act, IoT device vendors are required to implement security measures for each of their products and comply with the essential security requirements defined by the European Union—for example, by requiring clear disclosure of product-support periods and prohibiting the use of weak default passwords. When all necessary security measures have been implemented in a product, the CE mark label may be affixed to it to indicate conformity. Beginning in December 2027, IoT products without the label cannot be legally sold within the European Union.

> *Moving forward, coordination among like-minded countries and the development of interoperable international rules and norms will be essential to securing the global digital environment.*

This is a critical development because the efforts to regulate IoT security have already begun across multiple jurisdictions. Japan will launch its own voluntary certification system in 2025 through the **JC-STAR project**, managed by its Information-Technology Promotion Agency (IPA). The United States plans to introduce the **Cyber Trust Mark**, overseen by the Federal Communications Commission (FCC). The United Kingdom enacted the **Product Security and Telecommunications Infrastructure Act** in 2022; the act took effect in April 2024 and mandates basic security standards for consumer smart devices, including banning default passwords and requiring transparency on security support periods.

While these initiatives share the same goal—improving IoT security—their regulatory details differ. Moving forward, coordination among like-minded countries and the development of interoperable international rules and norms will be essential to securing the global digital environment.

ENSURING SECURE SOFTWARE DEVELOPMENT THROUGH THE SOFTWARE BILL OF MATERIALS (SBOM)

Software today is rarely built entirely from scratch. Instead, modern applications are each a collection of codes assembled from various sources—open-source libraries and proprietary components, to name a few. As both the scale and complexity of software development have grown exponentially, so too have the challenges of understanding and managing the software supply chain.

A striking example of this challenge emerged in late 2021, when researchers at Alibaba discovered a zero-day vulnerability, a critical software flaw unknown to the vendor at the time of discovery, in a widely used open-source library called Log4j. Until then, Log4j had been largely unknown outside the developer community. Log4j provides logging functionality, enabling software to record its own operational events. This particular library was popular because it allowed developers to easily add logging features without writing them from scratch. As a result, Log4j has been incorporated into countless products and services—including major platforms such as Cloudflare, Apple iCloud, Minecraft, Steam, Tencent QQ, and Twitter (now X).

The vulnerability in Log4j had an unprecedented impact on cybersecurity worldwide. A single flaw in this obscure software component suddenly exposed countless systems and users across the globe to potential exploitation. The real crisis, however, was not the vulnerability itself but rather the uncertainty it created: Few organizations could confidently say whether or where Log4j existed within their systems. As one cybersecurity expert described it: Log4j represented "**the single biggest, most critical vulnerability of the last decade.**"

The Log4j incident provided critical momentum for developing the Software Bill of Materials (SBOM) concept. Just as food packaging lists ingredients to inform consumers, software needs a similar mechanism to disclose its internal components. An SBOM provides this transparency, identifying the libraries—like Log4j—that are used within a piece of software.

The U.S. government has taken a leading role in promoting software supply-chain security. **A late-2021 executive order**, for example, mandated that software suppliers to the federal government provide SBOMs, effectively making them a requirement for government procurement contracts. These developments highlight the growing recognition—at least in the United States—that software supply-chain security is not only a technical issue but also a governance and policy priority. The continued leadership of the United States in this domain will remain critical in shaping the global conversation around SBOMs and secure software development.

The Japanese government and the country's various industries are facing challenges in responding to SBOM requirements. In particular, medical device manufacturers and companies in the automotive sector are conducting their own assessments to adapt to evolving requirements in the U.S. market. In response to this rapidly changing cyber ecosystem, the Ministry of Economy, Trade, and Industry (METI) published a document titled "**Guidelines on the Introduction of SBOM**" in July 2023, marking the beginning of efforts to create an environment that facilitates domestic companies' compliance with digital regulations.

Conclusion

Japan's cybersecurity is at a turning point. The scale and sophistication of threats from China, North Korea, and Russia continue to evolve. The country's Active Cyber Defense Bill represents a significant policy shift, reflecting Japan's growing recognition of cybersecurity as a core element of national security. Yet Japan's future efforts must extend beyond legislation and prioritize coordination with the United States and other like-minded countries. Strengthening cooperation to protect the public core of the internet, harmonizing IoT security standards, promoting secure software development, and deepening international cyber law enforcement collaboration will be essential to ensuring a resilient cyberspace—not only for Japan but for the entire international community. ■

Koichiro Komiyama *is director of the Global Coordination Division of the Japan Computer Emergency Response Team Coordination Center (JCERT/CC).*

This report is made possible with support from the government of Japan.