tentative translation

CYBERSECURITY STRATEGY

December 23, 2025

This Strategy is reported to the Diet pursuant to the provisions of Article 12, paragraph (4) of The Basic Act on Cybersecurity (Act No. 104 of 2014), as applied mutatis mutandis to paragraph (5) of the same Article.

Table of Contents

I. Background of Formulation

More than 30 years have passed since the start of the commercial use of the Internet in Japan. During this period, digital technology has undergone remarkable progress and widespread adoption, and cyberspace has become an indispensable foundation of our society and economy. Low-cost access to a wide range of services and information has become possible from anywhere in the world, bringing significant convenience to society. As cyberspace becomes more closely integrated with the physical world than ever before and comes to be described as another realm of reality, advanced technologies such as Artificial Intelligence (AI) and quantum technologies are poised to have a major impact on digital services and industries.

Meanwhile, in cyberspace, the threat of cyberattacks, in which the risk of exposure is relatively low and attackers have an advantage, is growing rapidly. This threat has also become a major concern in the context of today's complex international situation and the security environment surrounding Japan.

As the world marks 80 years since the end of World War II, the international order based on universal values such as freedom, democracy, respect for fundamental human rights, and the rule of law is facing an unprecedentedly severe crisis. This is due to the expansion of influence by states that do not share these universal values or the political and economic systems founded upon the values, as well as unilateral changes to the status quo by force and such attempts.

These impacts have extended into cyberspace, where cyberattacks have been used on an ongoing basis to disable or destroy critical infrastructures, interfere in foreign elections, demand ransoms, and steal sensitive information, even in the form of state-sponsored cyberattacks.

Furthermore, hybrid warfare, combining military and non-military means to achieve military objectives such as information warfare which utilizes the spread of disinformation prior to an armed attack, is being conducted. As the international situation becomes increasingly tense and the security environment grows more severe, the risk that cyberattacks will cause serious and potentially fatal damage to people's daily lives and economic activities is expected to continue to increase.

These risks must be addressed appropriately to for us to fully enjoy the value that cyberspace brings.

Japan's cybersecurity policy has reached a major turning point with the enactment of legislation enabling measures such as Active Cyber Defense.

Based on the "National Security Strategy" (decided by the National Security Council and approved by the Cabinet Decision on December 16, 2022), the "Expert Panel toward Improving Response Capabilities in the Field of Cybersecurity" was established in June 2024 to examine the development of legal frameworks and other measures aimed at strengthening

the response capabilities in the field of cybersecurity equal to or surpassing the level of leading Western countries.

Based on the recommendations by the panel compiled in November of the same year, the Act on Prevention of Harm Caused by Unauthorized Acts against Critical Computers (Act No. 42 of 2025; hereinafter referred to as the “Cyber Response Capability Strengthening Act”) and the Act on the Development of Related Laws Accompanying the Enforcement of the Act on the Prevention of Harm Caused by Unauthorized Acts against Critical Computers (Act No. 43 of 2025) (hereinafter collectively referred to, together with the Cyber Response Capability Strengthening Act, as the “Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts”) , which enables the introduction of Active Cyber Defense, were enacted in May 2025.

In addition, in July of the same year, following the partial enforcement of the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, the Cybersecurity Strategic Headquarters (hereinafter referred to as the “Headquarters”) was reorganized into a new structure, with the Prime Minister as its head and composed of all Ministers. At the same time, the “National Cybersecurity Office” was established within the Cabinet Secretariat as the control tower for ensuring cybersecurity across the public and private sectors, including national security in cyberspace.

Under this new structure, Japan’s efforts to ensure cybersecurity have entered a new phase. In order to promote Japan’s cybersecurity measures in an integrated manner through public-private and international collaboration, with the broad understanding and cooperation of the public and relevant parties, it is necessary to set out the goals and implementation policies of Japan’s various cybersecurity-related measures and present them domestically and internationally as a new Cybersecurity Strategy.

Based on the Basic Act on Cybersecurity (Act No. 104 of 2014; hereinafter referred to as the “Basic Act”), the Cybersecurity Strategy has been formulated roughly every three years since 2015. In this Cybersecurity Strategy, in order to promote in an integrated manner various initiatives to address threats surrounding cyberspace, including measures set out in “Urgent Matters to be Addressed to Deal with Threats Surrounding Cyberspace[1],” efforts based on the National Security Strategy, and initiatives under the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, the goals and implementation policies of measures to be undertaken over the next five years are set out from a medium- to long-term perspective.

[1] At the meeting of the Headquarters held on May 29, 2025, taking into account the “Cybersecurity Strategy” (Cabinet Decision on September 28, 2021), in particular, the “Measures to be taken especially strongly” set out in “Cybersecurity 2024” (decided by the Cybersecurity Strategic Headquarters on July 10, 2024), as well as the recommendations compiled by the “Advisory Panel for Improving Response Capabilities in the Field of National Security in Cyberspace”, the directions of measures requiring urgent action under the institutional framework in place prior to the enforcement of the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, were compiled.

Furthermore, the related measures stipulated in the Cyber Response Capability Strengthening Act be implemented in an integrated, effective, and appropriate manner, in conjunction with measures based on this Strategy, in accordance with the basic policy to be decided by the Cabinet and published pursuant to the same Act.

II. Fundamental Concept of the Strategy

1. The desired state of cyberspace and its basic principles

Japan has recognized cyberspace as the foundation for the sustainable development of the economy and society, as well as a foundation underpinning liberalism, democracy, and cultural development, and has sought to ensure “a free, fair and secure cyberspace” in order to contribute to the achievement of the purposes[2] set forth in the Basic Act.

In pursuit of this objective, the “Five Principles” (“assurance of the free flow of information[3],” “the rule of law[4],” “openness[5],” “autonomy[6],” and “collaboration among multi-stakeholders[7]”) have been set forth as the basic principles to be followed in the planning and implementation of cybersecurity-related measures.

Amid a serious crisis facing the international order based on universal values such as freedom, democracy, respect for fundamental human rights, and the rule of law, Japan reaffirms the importance of ensuring that cyberspace remains “a free, fair and secure space,” and of positioning the “Five Principles” as the basic principles for the planning and implementation of measures[8].

On the other hand, as the risk of cyber threats significantly impacting the daily lives of the Japanese people, economic activities, and, ultimately, national security continues to increase, there is a growing need for the government to play a more proactive role than ever before to

[2] “The purpose of this Act is to set a basic policy for Japan's cybersecurity initiatives, clarify things such as the responsibilities of the national and local governments, and provide for the formulation of a cybersecurity strategy and other things that will become the foundation of cybersecurity initiatives, and also to comprehensively and effectively advance cybersecurity initiatives in conjunction with the Basic Act on the Formation of a Digital Society (Act No. 35 of 2021) in ways such as establishing a Cybersecurity Strategic Headquarters, and by doing so, to enhance economic and social vitality and achieve sustainable development and bring about a society where the people can live with a sense of safety and security, and also to contribute to ensuring peace and safety in the international community and contribute to Japan's national security, in consideration of the context in which it has become an urgent issue to ensure cybersecurity while also ensuring the free flow of information, due to the increasing severity of threats to cybersecurity and other such changes in internal and external circumstances that are arising on a global scale as a function of the development of the Internet and other such advanced information and telecommunications networks, and the increased use of information and communications technologies(hereinafter referred to as ‘information and communications technologies’) prescribed in Article 2 of the Basic Act on the Formation of a Digital Society.” (Article 1 Basic Act).

[3] For the sustainable development of cyberspace as a place for creation and innovation, it is imperative to build and maintain a world in which transmitted information reaches the intended recipient without being unfairly censored or illegally modified in route. This is also necessary for the realization of “Data Free Flow with Trust,” which Japan promotes.

[4] As the integration of cyberspace and physical space progresses, the rule of law should be permeated in cyberspace, in the same way as in physical space as cyberspace developed as a foundation underpinning liberalism, democracy, and so forth. Similarly, it should also be made clear that any acts that threaten peace and activities that support such acts should not be condoned, on the premise that existing international law including the UN Charter is applied in the cyberspace.

[5] In order to achieve the sustainable development of cyberspace as a space to generate new values, it must be open to all stakeholders without restricting possibilities of linking diverse ideas and knowledges. In addition, Japan firmly adheres to the position that cyberspace must not be exclusively dominated by a certain group of stakeholders. This encompasses the idea that all stakeholders should be given equal opportunities.

[6] Cyberspace has developed through the autonomous initiatives of diverse stakeholders. It is inappropriate and impossible for a state to take on the entire role of maintaining order for cyberspace to sustainably develop as a space where order and creativity coexist. To maintain order in cyberspace, it is also important for various social systems to autonomously fulfill their roles and functions, thereby increasing society’s resilience as a whole and deterring the activities of malicious actors, so this will be facilitated.

[7] Cyberspace is a multi-dimensional world established through activities of diverse stakeholders, including the national and local governments, critical infrastructure operators, cyber-related and other businesses, educational and research institutions, and individuals. For the sustainable development of cyberspace, all stakeholders are required to consciously fulfill their respective roles and responsibilities. To do so, coordination and collaboration are required in addition to individual efforts. The government has the role of promoting this coordination and collaboration, while further promoting collaboration with other countries that share common values and cooperation with the international community, in light of changes in international situation.

[8] Given that Japan, together with other advanced democracies, should continue to uphold universal values such as freedom, democracy, respect for fundamental human rights, and the rule of law, “assurance of the free flow of information,” “the rule of law,” and “openness” continue to be important as the basic principles to be followed in the planning and implementation of measures. In addition, in order to ensure the security of cyberspace, which is formed by multi-stakeholders, autonomous efforts by each stakeholder and collaboration among multi-stakeholders are indispensable.

ensure “a free, fair and secure cyberspace” by adapting measures based on the “Five Principles” to today’s circumstances.

For instance, in cyberspace, where the “gray zone,” a broad spectrum of situations neither purely peacetime nor contingency, is expanding, Japan must engage in measures under public-private and international collaboration to detect sophisticated and advanced organized cyberattacks at an early stage and prevent damage. These measures include the collection and analysis of information, the proactive provision and dissemination of information, and the implementation of measures based on the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts. Many of these initiatives can only be undertaken by a national government, or achieve significant effects through the government’s active cooperation with various stakeholders.

Accordingly, while continuing to uphold the “Five Principles” as the basic principles to be followed in the planning and implementation of measures, Japan commits to strengthening measures and ensuring “a free, fair and secure cyberspace” in response to the increasingly severe situation surrounding cyberspace, with the government playing a more pivotal role than ever before.

Given the current environment surrounding Japan’s cyberspace, as outlined below, such proactive responses by the government will contribute to safeguarding “a free, fair and secure cyberspace” and the “Five Principles” (including “the rule of law”), which are currently threatened by severe cyberattacks. They will also support and strengthen efforts by a wide range of stakeholders to ensure cybersecurity based on principles such as “autonomy” and “collaboration among multi-stakeholders.”

2. Assessment of the environment surrounding cyberspace and future outlook

(1) An increasingly severe international environment and the rise of state-sponsored cyber threats

As Japan faces its most severe and complex security environment since the end of World War II, the landscape surrounding cyberspace, reflecting geopolitical tensions, has become increasingly challenging in recent years and carries the risk of rapidly developing into a grave crisis. In Japan as well, the number of cyberattack-related communications observed by the National Institute of Information and Communications Technology (NICT) has been increasing, and organized and sophisticated cyberattacks suspected of foreign state involvement have become apparent. As a result, the threat of cyberattacks has increased in both scale and sophistication, and the risk of serious and potentially catastrophic damage to the foundations of people’s daily lives and economic activities, and ultimately to the security of the nation and its people, has become real.

The countries and regions of particular note in the security environment surrounding Japan are also believed to be making state-level use of cyberattacks. Russia is believed to be using cyberattacks to achieve military and political objectives. It is alleged to have carried out attacks on the information systems and networks of Ukrainian government agencies and critical infrastructure operators prior to its aggression against Ukraine in 2022. This suggests that cyberattacks may be conducted as a preparatory step in anticipation of subsequent armed attacks. China is believed to be conducting cyberattacks to exfiltrate information from government agencies, critical infrastructure operators, and companies possessing advanced technologies. Recently, it has become clear that the China-backed group "Salt Typhoon" has been targeting the information systems and networks of telecommunications operators, government agencies and related agencies worldwide. Furthermore, as seen in cases in which the alleged China-backed group "Volt Typhoon" is reported to have used Living Off the Land (LOTL)[9] tactics to infiltrate the information systems and networks of U.S. military and government agencies, as well as critical infrastructure operators in Guam and other locations, and remained undetected for extended periods, assessments are emerging that China is conducting cyberattack campaigns[10] with a view toward disrupting or destroying the functions of critical infrastructure in anticipation of contingencies. Furthermore, North Korea generates illicit revenue through cryptocurrency thefts and the activities of IT workers dispatched abroad who obtain work with false identification. It has been pointed out that such revenue funds North Korea's nuclear and missile development, and that these IT workers are also highly likely to be involved in information theft[11]. It is also alleged to steal foreign classified military information and develop capabilities to attack the critical infrastructure of other countries. Against this backdrop, there is a growing recognition of the need to respond to cyberattacks with a sense of urgency, keeping in mind the possibility of contingencies.

In Japan as well, since 2019, the cyberattack group "MirrorFace," suspected of involvement by China, has been conducting cyberattack campaigns aimed at theft of information related to Japan's national security and advanced technologies[12]. In May 2024, North Korea-backed cyberattack group "TraderTraitor," stole cryptocurrency worth approximately 48.2 billion yen from a Japanese cryptocurrency–related business[13] [14].

[9] A cyberattack technique in which, after infiltrating a system, adversaries use legitimate administrative tools and functions built into the system to carry out activities such as credential theft and the collection of system information, thereby making detection difficult.
[10] Cyberattack activities repeatedly conducted over a certain period by a specific actor against specific organizations or sectors, such as a government or critical infrastructure, using specific attack methods and attack infrastructure.
[11] Publication of the Japan–U.S.–Republic of Korea "Joint Statement on North Korean Information Technology Workers" and the "Alert for Companies on North Korean Information Technology Workers" (August 27, 2025; National Police Agency, Ministry of Foreign Affairs, Ministry of Finance, and Ministry of Economy, Trade and Industry).
[12] "Regarding Cyberattacks by MirrorFace (Advisory)" (January 8, 2025; National Police Agency and National center of Incident readiness and Strategy for Cybersecurity).
[13] "Cyberattack Targeting Crypto-Asset-Related Business by North Korean Cyber Actor, TraderTraitor" (December 24, 2024; National Police Agency).
[14] The second report of the Multilateral Sanctions Monitoring Team (MSMT), published in October 2025, states that North Korea stole approximately USD 1.19 billion worth of cryptoassets in 2024 and approximately USD 1.65 billion worth by September 2025. It further notes that the majority of North Korea's foreign currency income in 2024 consisted of crypto-asset theft and arms sales to Russia. The report also indicates that North Korea is laundering the stolen cryptoassets through non-North Korean collaborators located in third countries to finance its nuclear and missile development programs.

Other incidents include a ransomware attack that brought operations at the Port of Nagoya to a halt (2023); an attack on the National center of Incident readiness and Strategy for Cybersecurity (NISC), believed to have been aimed at the theft of sensitive information (2023); and cyberattacks against the Japan Aerospace Exploration Agency (JAXA) (2021–2024).

In this way, sophisticated and advanced cyberattacks[15], including in the form of state-sponsored and targeting government agencies and critical infrastructure operators, have become national security threats that Japan is currently facing.

(2) Advancement of digitalization across society and the escalation of cyber threats

Through the COVID-19 pandemic and other developments that effectively accelerated the adoption of online services and telework, digital transformation (DX) across Japanese society as a whole has progressed significantly, including the use of IoT and cloud services.

As a result, while the efficiency and convenience of Japan's industries and services have improved significantly, the expansion and increasing complexity of supply chains have also heightened the risk that all entities, including individuals and small and medium-sized enterprises (SMEs), may become targets of cyberattacks. Not limited to direct damage, there is a risk that such incidents could develop into more serious attacks and lead to the expansion of damage through supply chain disruptions, the spread of leaked information, and the hijacking of IoT devices[16].

Furthermore, a broadening of the attacker base can be observed in current cyberattacks, as perpetrators no longer necessarily need to possess specialized technical expertise to carry out attacks. For example, cases have been confirmed in which entities that develop and operate ransomware provide ransomware and related tools to attack operators in exchange for a share of the ransom, a model known as Ransomware as a Service (RaaS). Just as there are individuals who trade authentication credentials used to infiltrate target companies' networks, there are cases in which multiple actors divide roles to carry out cyberattacks.

In the future, as digitalization continues to advance, reliance on digital services in people's daily lives and economic activities will increase further. At the same time, cyberattacks driven by various motives, including economic purposes, are expected to have increasingly severe impacts on people's daily lives, corporate activities, socio-

[15] With regard to state-sponsored cyberattacks, methodologies that make detection difficult, such as the Living Off the Land (LOTL) tactics described in footnote 9, have also been confirmed.

[16] For example, with regard to the suspension of corporate business activities and the spread of leaked information, in 2024, a major company engaged in publishing and other businesses suffered a large-scale cyberattack involving ransomware. As a result, its web services and other operations were suspended, and secondary damage occurred, including the leakage of personal and corporate information and its subsequent dissemination through social media and other channels. In addition, as examples of attacks targeting contractors and supply chains that led to business suspensions, in 2022 a business partner of a major automobile manufacturer was hit by a cyberattack (ransomware), resulting in the encryption of data on some servers and computer terminals and the temporary suspension of all of the manufacturer's plants in Japan. In the same year, a hospital was forced to temporarily suspend its regular medical services after suffering a cyberattack via a contracted catering service provider. As an example of large-scale distributed denial-of-service (DDoS) attacks, from late 2024 to early 2025, aviation operators, financial institutions, and telecommunications operators were subjected to a series of DDoS attacks, resulting in damage such as temporary service suspensions.

economic activities, and ultimately national security. In addition, new threats such as the increasing sophistication of cybercrime are emerging, and threats in cyberspace are expected to continue to grow in both quality and quantity.

(3) **Impact of new technological innovations, such as AI and quantum technology, on cybersecurity**

In the future, the rapid advancement of AI, including generative AI, has the potential to significantly enhance convenience and efficiency in industries and people's daily lives, while also giving rise to new threats such as the increasing sophistication of cybercrime. As AI becomes more widely adopted and utilized in society, attacks targeting AI and attacks leveraging AI are expected to intensify, emerging as new cybersecurity risks.

Furthermore, as the social implementation of quantum computers and quantum communication becomes increasingly realistic[17], a wide range of challenges must be addressed, including concerns over the deterioration of safety and potential compromise of currently widely used public-key cryptography as these technologies advance.

A timely and appropriate response is required to address the effects and impacts that these new technological innovations have on cybersecurity and national security.

Furthermore, to fully benefit from the advantages that these technological innovations bring to the field of cybersecurity, it is an urgent priority to develop and secure cybersecurity personnel and technologies to respond appropriately to their risks.

3. Key issues regarding cyberspace and policy directions

In light of the current situation Japan faces as described above, the following three issues can be identified with regard to cyberspace:

- Responding to cyber threats that seriously impact people's daily lives and economic activities in Japan, and ultimately, national security

Considering the risk that cyber threats could have a serious and potentially fatal impact on the daily lives of our citizens, economic activities, and ultimately national security, there is a need to effectively defend against cyberattacks through damage prevention and appropriate responses following incidents. On the other hand, as sophisticated and advanced cyberattacks, including state-sponsored cyberattack campaigns, are becoming increasingly apparent, it is difficult to completely defend Japan against all cyberattacks. Therefore, it is necessary to advance effective defense and deterrence efforts from the perspectives of national security and crisis management. This requires not only conventional defensive measures but also the persistent implementation of various response measures against attackers, including Active Cyber Defense, to

[17] Expert Panel on Quantum Technology Innovation, "Promotion Measures for the Development of a Quantum Ecosystem (Outline)" (May 30, 2025).

continuously impose costs on attackers on an ongoing basis and thereby deter cyber threats.

- Ensuring cybersecurity and resilience across society as a whole in response to the advancement and proliferation of digitalization and the accompanying expansion of risks

Given that, as digitalization advances across society, new technological innovations emerge, and supply chains become increasingly complex, all entities are exposed to cyberattacks and damage to or the suspension of operations at a single entity could have a major impact on society as a whole, it is necessary to raise the effectiveness of measures among a wide range of stakeholders that may become targets of attacks. To enhance the effectiveness of the aforementioned active defense and deterrence measures, it is necessary for individual entities to take appropriate measures, while Japan simultaneously promotes society-wide digitalization and the assurance of cybersecurity.

- Securing human resources and technologies that support Japan's cyber response and addressing advanced technologies

For effective defense and deterrence, as well as autonomous measures by individual entities, Japan needs to secure sufficient cybersecurity personnel and technologies. However, Japan faces a shortage of cybersecurity personnel across both the public and private sectors and remains dependent on overseas sources for many cybersecurity technologies. To address this issue, it is an urgent priority to establish an environment in Japan that sustainably develops the human resources and technologies necessary for cyber response. Furthermore, while advanced technologies such as AI and quantum technology are expected to be utilized in the field of cybersecurity, risks have also been identified, including concerns regarding the safety of AI, its potential malicious use for cyberattacks, and the deterioration of safety and potential compromise of existing public-key cryptography accompanying advances in quantum computing technology. Japan must take appropriate measures regarding such advanced technologies.

Based on the recognition of these challenges, Japan must respond appropriately to the pressing situation surrounding cyberspace, the spread of DX across society, and technological innovation in order to ensure "a free, fair and secure cyberspace." Through this, Japan seeks to achieve the objectives set forth in the Basic Act: "enhancing socio-economic vitality and sustainable development," "realizing a society in which people can live safely and with peace of mind," "ensuring peace and security in the international community," and "safeguarding Japan's national security." To this end, it is necessary to promote measures based on the following three directions:

- Defense and deterrence against intensifying cyber threats

- Enhancement of cybersecurity and resilience[18] across society by broad participation
- Formation of an ecosystem for human resources and technologies supporting Japan's cyber response capabilities

(1) Defense and deterrence against intensifying cyber threats

State-sponsored cyberattacks are organized and refined, sophisticated and advanced, and constitute a serious national security threat that Japan currently faces. Japan will collect information, including the utilization of communications data and under public-private and international collaboration, combine diverse means, including Active Cyber Defense made possible by the enactment of the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, in addition to damage prevention from cyberattacks and appropriate responses following incidents with the National Cybersecurity Office which serves as the control tower for Japan’s cybersecurity at the center, working in close coordination with the government agencies and related agencies to respond flexibly and appropriately to the severe security environment in cyberspace. Through these efforts, Japan will continuously impose costs on attackers on an ongoing basis and proactively defend against and deter cyber threats targeting the nation.

In undertaking these efforts, it is necessary for the government to take the lead in advancing initiatives, including measures based on the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts. However, this cannot be achieved by the government alone; rather, the government must play a proactive role in promoting collaboration among multi-stakeholders.

(2) Enhancement of cybersecurity and resilience across society by broad participation

Enhance the cybersecurity and resilience of society as a whole by calling on a wide range of stakeholders that could become targets of attacks to take appropriate measures, based on their own capabilities and the risks posed by the attacks to society.

First, government agencies and related agencies should lead by example by implementing robust measures. At the same time, the government should clarify the measures required of a wide range of stakeholders and swiftly implement them, together with strategies to ensure their effectiveness. These stakeholders include not only critical infrastructure operators and local governments, but also cyber-related businesses and vendors that play a significant role in ensuring cybersecurity, as well as SMEs and individuals. Through these efforts, Japan will simultaneously promote society-wide digitalization and the assurance of cybersecurity.

In undertaking these initiatives, various social systems are expected to autonomously fulfill their respective missions and functions with regard to cybersecurity, and the

[18] This refers to mechanisms, capabilities, and resilience that minimize the impact of an incident and enable rapid restoration to the original state.

government will provide support and develop the necessary environment to promote such efforts by each stakeholder.

(3) Formation of an ecosystem for human resources and technologies supporting Japan's cyber response capabilities

Across industry, academia, and government, Japan will focus more than ever on securing, developing, and broadening the base of cybersecurity personnel. Furthermore, Japan will form an ecosystem that generates new technologies and services centered on technologies and services developed in Japan through cross-sector collaboration spanning industry, academia, and government, from research and development to implementation and operation. It will also prepare for and respond to transformations in the cybersecurity field brought about by new technological innovations such as AI and quantum technology.

In this regard as well, in light of the fact that human resources and technologies in the cybersecurity field have not been sufficiently developed in Japan to date, the government will play a more proactive role, while respecting the “autonomy” of each relevant stakeholder and promoting “collaboration among multi-stakeholders.”

There are limits to implementing these measures through the public sector alone, the private sector alone, or a single country alone. Under public-private and international collaboration, with a broad understanding from the public and relevant stakeholders, the government will take the lead in advancing Japan’s cybersecurity measures in cooperation with the public and private sectors.

Through these efforts, Japan aims to become a nation with world-class resilience capable of responding seamlessly to the increasingly severe situation surrounding cyberspace.

Furthermore, in promoting measures based on this Strategy, due consideration should be given to the following points.

- To ensure cybersecurity across Japan as a whole, seamless efforts are required, ranging from responses based on a perspective of national security in cyberspace to cyber threats targeting government agencies and critical infrastructure operators, to proactive and autonomous measures by individuals and companies, as well as initiatives that support such efforts. These efforts are mutually complementary. Furthermore, as cyberspace has no borders, cybersecurity measures should be advanced in an organically coordinated manner. This Strategy aims to enhance the effectiveness of measures by implementing the necessary measures seamlessly in an integrated and comprehensive manner.
- With advances in generative AI technology and other factors, there are growing concerns about the increasing threat of influence operations, including the dissemination of disinformation from abroad via cyberspace. This issue could affect the foundations of Japan’s sound democracy and may also be carried out in conjunction with cyberattacks.

In light of these circumstances, the relevant ministries and agencies involved in the issue will work in close coordination and take appropriate and necessary measures based on this Strategy, from the perspective of ensuring Japan's cybersecurity.

- It is necessary to gain public awareness and understanding regarding the actual state of threats in cyberspace, as described above. In promoting national responses and measures, including active defense and deterrence measures based on the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, the government will strive to obtain broad public understanding and cooperation while working in coordination with relevant stakeholders.

III. Measures for Achievement of the Objectives

This section, taking into account the situation surrounding Japan and the recognition of cybersecurity-related challenges described above, sets out the goals and implementation policies for measures to be undertaken over the next five years under the three major policy pillars presented in II.3, in order to achieve the objectives set forth in the Basic Act and ensure "a free, fair and secure cyberspace."

1. Defense and deterrence against intensifying cyber threats

State-sponsored organized and refined cyberattacks are being carried out by exploiting zero-day vulnerabilities and leveraging multi-layered combinations of numerous servers both within Japan and internationally. Such attacks have become sophisticated and advanced, and constitute a serious national security threat that Japan is currently facing.

Furthermore, cyberattacks are characterized by the lack of a clear distinction between peacetime and contingency, and can easily escalate. It must be assumed that cyberattacks against government agencies, critical infrastructure operators, and other entities may be conducted in the preparatory stages of an armed attack against Japan, and that cyberattacks may continue even after the outbreak of an armed attack as part of hybrid warfare combined with military and physical means.

In order to respond flexibly and appropriately to such an increasingly severe security environment in cyberspace, Japan will further strengthen information collection and analysis capabilities in the field of national security in cyberspace, particularly with regard to adversaries behind cyberattacks, including state-sponsored actors, so as to accurately grasp the situation, defend against cyberattacks targeting Japan, and deter threats of cyberattacks from reaching the country, with the goal of preventing damage before it occurs or preventing the expansion of damage. To this end, while enhancing these capabilities, it is essential to fundamentally strengthen the government's overall ability to respond seamlessly.

The "National Security Strategy" of 2022 set the objective of "the response capabilities in the field of cybersecurity should be strengthened equal to or surpassing the level of leading Western countries" in order to ensure secure and stable use of cyberspace, in order to ensure secure and stable use of cyberspace, especially the security of government agencies and critical infrastructure operators. As a concrete measure, Japan decided to introduce Active Cyber Defense in order to prevent damage from cyberattacks that may cause national security concerns to government agencies and critical infrastructure. The strategy also states that, in addressing Japan's defense challenges, it is necessary to utilize not only its defense capabilities but also its comprehensive national power. It calls for the promotion of efforts of national security in cyberspace, including Active Cyber Defense, that complement and are inseparable from the fundamental reinforcement of defense capabilities, thereby reinforcing its comprehensive defense architecture.

Active Cyber Defense is built on three pillars: (i) strengthening public–private collaboration, with the government playing a more proactive role in ensuring cybersecurity through integrated public–private efforts; (ii) utilizing communications data to detect the sources of cyberattacks within increasingly complex networks; and (iii) introducing measures whereby government agencies access servers and other systems that serve as sources of cyberattacks and neutralize threats (remote access and neutralization measures).

In addition to reinforcing existing cybersecurity measures on the defensive side, such as information collection from victimized companies and response support, Japan will, through a range of measures to counter attackers, including Active Cyber Defense, build a posture that seamlessly defends the nation by continuously imposing costs on attackers on an ongoing basis. These efforts will contribute to strengthening Japan's comprehensive defense posture.

Accordingly, in the future, Japan will treat measures on the defensive side and measures to counter attackers as "two sides of a coin," and will seek to comprehensively enhance its cyber defense capabilities, with the aim of continuously imposing greater costs on attackers on an ongoing basis.

In addition, Japan will strengthen the formation of a public–private collaboration ecosystem and reinforce cross-cutting measures based on trust and cooperative frameworks between the public and private sectors. Recognizing that it is difficult for a single country to address increasingly serious cyber threats alone, Japan will further promote and strengthen international collaboration.

Through these efforts, and in order to achieve the above objectives, the public and private sectors will work together, including through necessary investments, to implement the following measures organically and efficiently under the comprehensive coordination of the National Cybersecurity Office.

(1) Defense and deterrence, with the government playing pivotal roles

In order to protect cyberspace from sophisticated and advanced cyberattacks, including state-sponsored ones, the National Cybersecurity Office, serving as the control tower, will play a pivotal role in coordinating with relevant ministries, agencies, and specialized organizations. Through the combination of diverse measures, including Active Cyber Defense, Japan will promote initiatives toward effective defense and deterrence, incorporating national security considerations, including the elimination of threats before damage occurs and appropriate responses following the occurrence of incidents.

To date, the government has performed functions as the national CERTs/CSIRTs, working to ensure swift and appropriate incident response and to prevent damage. Through initiatives to streamline and strengthen information collection, analysis, provision, and dissemination, Japan will further enhance these functions while leveraging information collection and sharing frameworks that have been reinforced under the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts.

In addition, cybersecurity-related information, including communications data acquired under the Cyber Response Capability Strengthening Act, as well as information accumulated through public–private collaboration and international collaboration, will be consolidated, analyzed and provided appropriately to entities that require such information.

The government will promptly establish and strengthen the implementation framework for various measures to counter attackers, including remote access and neutralization measures.

At the same time, Japan will promptly and comprehensively develop and operate the necessary systems, infrastructure, and human resources required to implement these initiatives effectively, drawing on examples from other countries.

(i) Preventing the expansion and escalation of damage through advanced incident response

The ability to respond promptly and effectively to incidents caused by cyberattacks, including initial response, investigation, and root cause analysis, is essential to preventing the expansion and escalation of damage. Such responses must be further strengthened by leveraging the new framework established under the Cyber Response Capability Strengthening Act.

The National Cybersecurity Office, performing functions as the national CERTs/CSIRTs, conducts prompt and appropriate identification, analysis, and evaluation of incidents. In the event of an incident, the Office coordinates with relevant ministries, agencies, and specialized organizations to issue timely and appropriate alerts and disseminate information to organizations in Japan and the public, with the aim of preventing damage.

To support prompt initial response, the government will, pursuant to the Cyber Response Capability Strengthening Act, establish an information sharing platform to notify the government of specified critical computers and to report incidents by essential infrastructure service providers (specified essential infrastructure service providers under the Economic Security Promotion Act[19]) and other relevant entities. Furthermore, in order to enable private-sector companies to share information with confidence, the government will undertake appropriate measures to ensure the proper protection of information. Furthermore, to enable affected organizations to focus on response activities, the government will seek to reduce the burden associated with the standardization of reporting formats, including those required under the Cyber Response Capability Strengthening Act, and by advancing necessary coordination toward the centralization of reporting channels.

With regard to information dissemination for the prevention of damage, the government will employ a “single voice” approach to ensure that there are no discrepancies in content among agencies. There is growing concern over the exploitation

[19] Act on the Promotion of Ensuring National Security through Integrated Implementation of Economic Measures (Act No. 43 of 2022)

of system and software vulnerabilities by organizations suspected of being state-sponsored actors, increasing the need for a government-led response. To this end, the government will organize and analyze the vulnerability information it collects and take the lead in providing private businesses and other entities with information that is effective in preventing damage. Furthermore, vendors (suppliers of computers[20]) will be encouraged to implement necessary measures to prevent damage from cyberattacks, including through requests for action by the competent minister under the Cyber Response Capability Strengthening Act.

Additionally, in the case of large-scale incidents, a unified, response of government agencies and related agencies will be necessary to prevent the expansion and escalation of damage, in addition to responses by individual government agencies. Accordingly, the government will develop frameworks to enable swift and appropriate initial response and also conduct practical exercises to enhance incident response capabilities in cooperation not only with government agencies and related agencies, but also with critical infrastructure operators, local governments, and other relevant organizations.

(ii) Aggregation, effective analysis, and utilization of cybersecurity-related information, including communications data

To effectively counter cyberattacks, it is necessary to detect them at an early stage and analyze their patterns, including the characteristics of the adversaries.

Under current circumstances, however, even when an attack is detected, only fragmented data/information can be obtained, making it difficult in many cases to conduct analyses that contribute to the prevention of damage. Accordingly, in addition to publicly available information on cyberattacks, the government will consolidate at the National Cybersecurity Office all data/information useful for analysis, including damage reports, such as incident reports submitted by essential infrastructure service providers and other entities pursuant to the Cyber Response Capability Strengthening Act; data/information shared through cooperation with its ally and like-minded countries; data/information obtained through the monitoring and analysis of government agencies and related agencies' terminals; and data/information acquired through observation of cyberspace[21]. Each ministry and agency is required, in collaboration with the National Cybersecurity Office, to collect data/information on incidents occurring within its respective remit, giving due consideration to the response status of affected organizations. Such information will then be shared with the Office for use in the analysis of cyber threats. Relevant organizations, such as the Information-technology Promotion Agency, Japan (IPA), will also continue, with the consent of affected organizations, to share all incident and analysis data/information they collect with the Office.

[20] "Suppliers of computers" refers to persons who supply computers or the computer programs (computers to be used as critical computers or computer programs to be installed on the computers), including persons who provide services enabling others to use computers or the programs, for information processing (Article 42(1) of the Cyber Response Capability Strengthening Act).
[21] For example, the Network Incident Analysis Center for Tactical Emergency Response (NICTER) project led by NICT.

In particular, in organized and sophisticated cyberattacks suspected of involvement by foreign states, it is confirmed that attackers employ techniques designed to conceal the source of their attacks, making it extremely difficult to detect and track attack-related communications using conventional means of data/information collection[22]. Such cyberattacks often go unrecognized by victim organizations, which in many cases fail to submit incident reports to the government. Accordingly, the government will further strengthen the collection and consolidation of data/information on cyber threats by utilizing communications data newly made available under the Cyber Response Capability Strengthening Act, with the aim of identifying potential damage and gaining an understanding of attack patterns.

From the perspective of ensuring the security of the state and the people, communications data will be analyzed for the purpose of preventing cyberattacks from disrupting the essential functions of the government, essential infrastructure service providers, and other entities, while ensuring strict handling of such data/information with due regard for the secrecy of communications and enabling its effective use in the implementation of remote access and neutralization measures. In doing so, the specialized expertise of the relevant ministries and agencies such as the Ministry of Defense will be utilized.

Furthermore, in addition to cyber-related data/information, the government will, with the cooperation of relevant ministries, agencies, etc., leverage national security information, including geopolitical developments outside the domain of cyberspace, to analyze attacker intent and objectives, the extent of involvement by foreign states, and linkages between cyberattacks and real-world events, with a view to utilizing such analysis in remote access and neutralization measures. At the same time, a framework will be established for the regular analysis and assessment of threats to Japan, thereby fundamentally enhancing national cyber analysis capabilities.

To develop this framework, the government will promote efforts to increase the number of analysts and enhance their capabilities within the National Cybersecurity Office and other relevant ministries, agencies, etc., introduce equipment and systems incorporating AI and other cutting-edge technologies from various countries, and improve facilities. The government will also promote active collaboration, including cooperation with private-sector cybersecurity analysts, in conducting analyses.

The government will actively share the results of analyses within the government, its allies and like-minded countries, with parties to new agreements concluded under the Cyber Response Capability Strengthening Act, with members of the new council established under this Act (hereinafter referred to as the “New Council”), and with users and vendors (suppliers of computers) of critical computers. It will promote two-way information sharing among government entities and between the public and private

[22] Techniques include disguising malicious activity as normal traffic to make detection by victim organizations more difficult, as well as constructing multi-layered architectures composed of numerous botnets and command-and-control (C2) servers, by hijacking the communications devices of ordinary users.

sectors, thereby establishing an information ecosystem and increasing the cyber resilience of society as a whole. In such cases, information is required to be provided appropriately in accordance with the laws and regulations and based on the principle of Need to Share[23], while ensuring proper handling of information based on the basic concept of information protection, including the principle of Need to Know[24].

(iii) Active defense and deterrence through a combination of multiple measures, including remote access and neutralization measures

To address routine and persistent cyberattacks, including state-sponsored cyberattack campaigns, Japan must respond proactively and steadfastly by employing a diverse range of means that combine its existing defensive efforts with new Active Cyber Defense measures, including remote access and neutralization measures. To this end, the government will establish and strengthen the necessary structure at an early stage.

Specifically, when there is the possibility of serious cyberattacks that may cause national security concerns, even if they do not amount to an armed attack, the government will implement remote access and neutralization measures as far as permitted under international law, by directly engaging with attackers' servers and other infrastructure in order to prevent damage from such attacks. These measures also serve to deter threats of cyberattacks. As their implementation requires the full mobilization of Japan's national capabilities, a joint response structure will be established in which the police, possessing advanced forensic capabilities, including malware analysis, as well as sophisticated intelligence analysis capabilities to identify attackers and cyberattack methods, will work in close coordination with the Ministry of Defense (MOD) and the Self-Defense Forces (SDF), which possess advanced cyber defense capabilities to counter high-intensity cyberattacks in situations such as armed attacks.

These measures must be implemented in a manner coherently aligned with national security considerations, ensuring seamless responses from peacetime through contingencies. Under the leadership of the Minister of State for Cybersecurity[25], the National Cybersecurity Office, serving as the control tower, will exercise comprehensive coordination functions in close cooperation with the National Security Secretariat. Under a unified policy, a structure will be established to enable the police and the MOD/SDF to implement these measures appropriately and efficiently. In addition, the National Cybersecurity Office will maintain close coordination with relevant ministries and agencies on an ongoing basis through information sharing, liaison, and exchanges of views. To ensure operational coordination, particularly between the police and the MOD/SDF, which are responsible for implementing remote access and neutralization measures, it will develop an operational environment that includes new hubs dedicated to handling cyberattacks.

[23] The principle that information should be proactively shared with necessary stakeholders and relevant communities.
[24] The principle that information should be shared only with individuals who have a need to know and are in a position to know.
[25] The Minister of State responsible for promoting national security in cyberspace and ensuring cybersecurity.

It is necessary to substantially strengthen the capabilities of relevant administrative agencies, particularly those of the police and the MOD/SDF, which are responsible for implementing these cybersecurity measures. In addition to strengthening the structures of relevant departments and units, the government will, following careful consideration, expeditiously advance the development and securement of necessary systems and equipment, as well as operational environments, with due regard to ensuring seamless responses from peacetime through contingency.

Furthermore, by combining the new public–private collaboration framework established under the Cyber Response Capability Strengthening Act with existing initiatives, the government will actively provide cyber threat information and other intelligence on attacks employing advanced intrusion and stealth capabilities to private businesses and other entities, taking into account their information needs. This will enable private businesses and other entities to take concrete actions, thereby contributing to the prevention of damage from cyberattacks.

In addition to the initiatives based on the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, conventional measures, including voluntary takedowns conducted in coordination with administrators of servers and other infrastructure, public attribution, and the disclosure of attack methods, are extremely important. To deter the threat of serious cyberattacks and prevent damage caused by them, the government will consider and implement all available options, not limited to measures based on the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, under comprehensive coordination of the National Cybersecurity Office, while ensuring close cooperation with relevant ministries and agencies.

To implement the above active defense and deterrence initiatives, joint training and exercises will be conducted among relevant ministries, agencies, etc., and the sharing of insights and lessons learned based on the results will be steadily advanced. In addition, the government will actively consider the use of advanced technologies, including AI, for the development and securing of systems and equipment, while striving to fully leverage the high-level capabilities of private businesses.

Given the cross-border nature of cyberspace, where the impact of incidents readily transcends national boundaries, and the difficulty for any single country to address sophisticated cyberattacks alone, effective international collaboration and cooperation with its ally and like-minded countries in the cyber field are of critical importance. In particular, when considering and implementing various measures related to active defense and deterrence, such as remote access and neutralization measures and public attribution, Japan will, as appropriate, share necessary information and pursue coordinated responses with its ally and like-minded countries, while actively contributing to multilateral discussions aimed at shaping international frameworks and rules.

(iv) Comprehensive development and operation of frameworks, infrastructure, and human resources, etc.

To work sustainably and effectively toward ensuring our national security in cyberspace, the government will comprehensively develop the necessary systems, infrastructure, and human resources, while promoting the planning and implementation of related policies and strengthening the cyber response and incident handling capabilities. In addition, should operational issues or challenges arise, relevant measures will be promptly reviewed and improved in order to respond appropriately to increasingly serious cyber threats. To this end, the National Cybersecurity Office, serving as the control tower, together with ministries responsible for critical and essential infrastructure, ministries implementing remote access and neutralization measures under the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, and ministries promoting cybersecurity policies, will strive to develop and strengthen their respective systems and frameworks. Additionally, cooperation will be promoted not only among government agencies but also with public-sector affiliated organizations [26], private organizations [27], and private businesses, in order to comprehensively develop the systems, infrastructure, and human resources required to support advanced information gathering and analysis capabilities.

With respect to the Japan Active Cyber Defense Oversight Commission, which will be established as an independent body to ensure the proper use of communications data and the appropriate implementation of remote access and neutralization measures, the relevant division in the Cabinet Secretariat will proceed with preparations for the development of the necessary systems and related measures. Following this, the Commission will ensure that the authorities granted to it under the Cyber Response Capability Strengthening Act, such as the granting of appropriate approvals and the conduct of inspections, are exercised effectively, thereby ensuring proper enforcement of the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts. In this regard, in order to ensure the smooth implementation of these procedures and enhance the effectiveness of the Act, the Commission will review its operations, drawing on examples from other countries. At the same time, relevant ministries and agencies, including the National Cybersecurity Office, will, on an ongoing basis, proactively share with the Commission relevant information, such as the cybersecurity situation and related assessments, and strive to foster a shared understanding and maintain effective communication.

(2) Formation of a public–private collaboration ecosystem and strengthening of cross-sectoral measures

As cyberattacks become sophisticated and advanced, there are limits to defense efforts

[26] Such as NICT and IPA

[27] Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), Japan Cybercrime Control Center (JC3), and Information Sharing and Analysis Center (ISAC: an organization that collects and analyzes cybersecurity-related information).

undertaken solely by either the government or the private sector. Accordingly, the government and the private sector must work in close collaboration, acting as one, to enhance Japan's overall cyber defense capabilities.

First and foremost, the government and the private sector must deepen their mutual understanding as trusted partners, encompassing both the corporate perspective, that cybersecurity measures constitute a critical management issue that is central to a company's survival, and the national perspective, that cybersecurity measures are directly linked to national security, specifically, ensuring the safety of Japan as a whole and securing the autonomy and indispensability of the country's industrial and technological foundation.

In addition to strengthening incident response capabilities with a focus on the victim side, the government and the private sector will share a common understanding of the direction Japan should pursue in ensuring cybersecurity, namely, strengthening the nation's overall cyber defense through public–private collaboration and implementing active defense and deterrence measures to counter attackers.

To this end, the government seeks to establish a new public–private collaboration ecosystem founded on a cycle of two-way, proactive information sharing and response measures, under which the government and the private sector work together in close cooperation.

Specifically, the government will analyze threats in cyberspace, taking into account information provided by private-sector companies, and will proactively share relevant information with private-sector entities by utilizing the frameworks of the New Council described below. In the event of an incident, the government will, taking into account incident information received from government agencies, private-sector companies, and other sources, issue advisories to prevent the spread of damage.

Utilizing such information provided by the government, private-sector companies will implement appropriate response measures, and in turn, share relevant information they possess with the government.

In addition to establishing this cycle of information sharing and response measures, Japan will further enhance cross-cutting measures across the public and private sectors, including risk assessments aimed at strengthening private-sector response measures, more expanded implementation of threat hunting by both the government and the private sector, and continuous improvement through the systematic conduct of exercises, thereby enhancing cybersecurity capabilities across both sectors and strengthening overall national resilience.

(i) Formation of a public–private collaboration ecosystem and strengthening of cross-sectoral measures

In order to foster the shared understanding and relationship of trust that underpin public–private collaboration, it is necessary for the public and private sectors to engage

continuously in multilayered dialogue. Such dialogue will be pursued from multiple perspectives, involving participants from operational staff to senior management, and conducted at different levels, either individually or on a cross-sectoral basis, as necessary.

To enable private-sector management -- who are responsible for an organization's overall direction and strategy -- to recognize the long-term risks and business importance of cybersecurity measures and to make management decisions from a broader security perspective, the government will engage in regular exchanges of views with private-sector management and proactively share relevant threat-related information, analyses, and measures (hereinafter referred to as "threat information"), based on their needs. Furthermore, the government will proactively provide practical information, including trends in technical threats, specific attack techniques, and response methods, in order to enable operational personnel at the forefront of cybersecurity to implement response measures effectively with the understanding and support of management.

Rather than attempting to coordinate for the first time during an emergency, the government will seek to build trusted relationships on an ongoing basis, building a framework that enables effective, unified responses to unpredictable cyberattack threats. To this end, the New Council will be established in the fall of 2026, with a view to building a new public–private collaboration ecosystem. The New Council will comprise, among others, essential infrastructure service providers that support the daily lives and economic activities of Japanese people, operators handling sensitive information, security vendors, and government agencies and related agencies . Under the comprehensive coordination of the National Cybersecurity Office, the Cabinet Office will facilitate the mutual sharing of threat-related information among members, both during normal times and in the event of an incident.

Based on the needs identified by members of the New Council, the Cabinet Office will conduct analyses using information available exclusively to the government, including incident reports; registered asset information from essential infrastructure service providers; asset information and GSOC[28] log data from relevant government agencies and related agencies; and information shared by domestic specialized agencies and foreign authorities. By proactively sharing relevant threat information with members based on these analyses, the government will work toward enhancing members' motivation to participate in the New Council, and foster the creation of a sustainable and evolving community within the Council. To this end, the government will work to expand information resources and analytical capabilities, identify needs through regular communication with members, and establish a platform for two-way information sharing

[28] GSOC is an abbreviation for the Government Security Operation Coordination Team. It refers to a team responsible for cross-government information security monitoring and rapid response coordination across government-related organizations. The GSOC system, which enables cross-government monitoring through sensors installed in each agency and cloud-based monitoring, supports the analysis and investigation of cyberattacks and other incidents, the provision of advice to individual agencies, the promotion of inter-agency collaboration, and information sharing. The first GSOC team (established within the National Cybersecurity Office) began operations in April 2008 to monitor government agencies, while the second GSOC team (established within the Information-technology Promotion Agency (IPA)) began operations in April 2017 to monitor incorporated administrative agencies.

in order to promote information exchange within the New Council.

Additionally, the government will provide, as necessary and as appropriate, highly sensitive threat information to members through a security clearance system. The National Cybersecurity Office will lead the coordination in promoting the use of this system[29].

Moving forward, the government will work toward developing the New Council in phases by equipping it with functions such as offering public–private collaborative projects, taking into account the needs of participating companies and other relevant stakeholders.

In addition, providing unclassified information to stakeholders other than members of the New Council should help contribute to strengthening cybersecurity across Japan.

Leveraging the insights and outcomes gained from large-scale international events, such as Expo 2025 Osaka, the government will, in cooperation with relevant organizations, support cyber-incident-response and consultation, and thus risk assessments, with a view to strengthening private-sector measures, for future events, including the International Horticultural Expo (Green Expo) 2027.

(ii) Expanding threat hunting activities across the public and private sectors

In recent years, public and private organizations in Japan have been the target of advanced cyberattacks, such as Living Off the Land (LOTL) tactics. These attacks pose a threat from actors (hereinafter referred to as “advanced threat actors”) that adversely impact Japan’s economy and society, citizens’ daily lives, and ultimately national security.

While it goes without saying that the proper implementation of existing cybersecurity measures is important, many such cyberattacks are designed to evade existing cybersecurity measures. Under these circumstances, it is necessary for Japanese organizations to implement “threat hunting,” a method for detecting damage from cyberattacks by actively searching for traces of attacks that have evaded detection and infiltrated or remained dormant within systems. Threat hunting also serves as an effective means of obtaining information to support Active Cyber Defense, including remote access and neutralization measures. The need for threat hunting is recognized as being particularly high among government agencies, incorporated administrative agencies, and private businesses that are critical to ensuring national security in cyberspace and are likely targets of advanced threat actors. Accordingly, the government will formulate a basic policy about spread promotion and implementation of threat hunting around the summer of 2026.

On that basis, various measures aimed at enhancing cybersecurity capabilities will be implemented, with due consideration given to the following points.

First, in light of the current situation in Japan, where threat hunting has not yet become

[29] In applying the security clearance system, consideration will also be given to secondary effects, such as the potential for clearance holders to gain opportunities to participate in international communities.

widespread, its adoption must be promoted. The government must promote the implementation of threat hunting by raising awareness of its importance, clarifying its definition, establishing methodologies that leverage advanced technologies, and organizing initiatives in accordance with differing needs, capabilities, and organizational frameworks.

Next, the government must clearly position threat hunting as a means for implementing Active Cyber Defense and clarify its expected roles. In addition, to ensure its effectiveness, it is necessary to continuously strengthen threat-hunting capabilities within relevant organizations, with support for such efforts provided by the National Cybersecurity Office.

Furthermore, as the effectiveness of threat hunting is enhanced through information sharing among organizations, it is important to promote both public–private information sharing and international collaboration.

In advancing these initiatives, the government will consider how to leverage the threat-hunting capabilities of the police and the MOD/SDF for use by government agencies, incorporated administrative agencies, and private businesses that are critical to ensuring national security in cyberspace.

(iii) Systematic implementation of cybersecurity exercises

To enhance practical response capabilities in incident management, it is essential to conduct exercises based on realistic and up-to-date threat trends and to verify the effectiveness of response frameworks. Furthermore, exercises contribute to promoting mutual understanding and building relationships of trust among participants, and can be utilized to strengthen public–private collaboration and international collaboration. At present, cybersecurity-related exercises are conducted by various stakeholders across different sectors. However, as coordination among individual exercises remains limited, it is essential to maximize their effectiveness by appropriately allocating roles among the various exercises according to their objectives and scale, with due consideration given to efficiency and rationality. To this end, the government will conduct exercises in a systematic manner, bearing in mind the importance of continuously strengthening the public–private collaboration ecosystem and international collaboration. This will enable efficient and effective cross-sectoral implementation of exercises, promote the mutual sharing of know-how and outcomes from these exercises, and enhance national resilience through the exercises.

(3) Promoting and strengthening international cooperation

Cyberattacks are characterized by anonymity, asymmetry, and a cross-border nature, and in recent years, their attack methods have become sophisticated and advanced. As no state can effectively respond to such cyberattacks on its own, the promotion of international collaboration constitutes a cornerstone of Japan’s cybersecurity policy.

Based on this recognition, Japan will seek to enhance its cyber analysis and response capabilities by strengthening information and operational cooperation with its ally and like-minded countries, while actively participating in international efforts aimed at deterring malicious cyber activities.

Furthermore, given that the stability and prosperity of the Indo-Pacific region constitute the basis of Japan's development, Japan will promote support to enhance response capabilities in the region.

In addition, Japan will contribute to the maintenance and development of the international order in cyberspace by actively participating in international rule-making in collaboration with ally and like-minded countries and reflecting Japan's basic philosophy therein.

By promoting these efforts in an integrated and comprehensive manner, Japan will play a responsible and leading role in the international community and realize "a free, fair and secure cyberspace."

(i) Cooperation with allies, like-minded countries and others in information and operational domains

In response to intensifying cyberattacks, it is important to promote multi-layered cooperation and collaboration at various levels, including governments of various countries and the private sector, encompassing both information and operational aspects.

Japan will maintain continuous dialogue with relevant institutions in its ally and like-minded countries. In addition to policy best practices, Japan will promote information cooperation that contributes to enhancing its cyber analysis and response capabilities by appropriately sharing technical information related to cyberattacks, such as vulnerability information, Indicator of Compromise (IoC[30]) information, and attack methods, as well as information on the background and objectives of cyberattacks. In doing so, necessary information security measures will be thoroughly implemented.

In multilateral frameworks, Japan will strengthen cooperation within frameworks such as the Quad (Japan-U.S.-Australia-India), Japan-U.S.-ROK, and Japan-ASEAN, as well as in multilateral meetings related to threat response, including the Counter Ransomware Initiative (CRI)[31] and networks between international CERTs.

Furthermore, Japan will continue to promote international joint investigations and actively work to establish cooperative relationships with investigative agencies in multilateral settings, including by further strengthening collaboration with INTERPOL and EUROPOL, in order to deter cyber threats through arrests.

Furthermore, to deter malicious cyber activities, Japan will develop the capability to take international leadership in initiatives such as public attribution, including the

[30] Indicator of Compromise. Information that provides clues to determine whether an attack occurred against the system and what tools were used.

[31] Counter Ransomware Initiative A multilateral forum established in October 2021 under U.S. leadership, focused on international collaboration against ransomware. As of October 27, 2025, 74 countries and organizations have joined, discussing measures against ransomware, awareness-raising activities, and sharing threat information.

identification and public disclosure of threat actors, as well as the publication of international technical documents compiling technical information on malicious cyber activities. These efforts will be promoted in close coordination with its ally and like-minded countries, including through diplomatic responses. In addition, with regard to the consideration and implementation of various measures related to active defense and deterrence, Japan will appropriately coordinate with its ally and like-minded countries and enhance cooperation with relevant agencies at the operational level.

(ii) Support and promotion of enhanced cybersecurity response capabilities in the Indo-Pacific region

As cyberattacks transcend borders, the national security environments of other countries, including those in the Indo-Pacific region, are directly linked to policy of Japan's national security in cyberspace. Therefore, by supporting and promoting the enhancement of response capabilities in the field of national security in cyberspace, Japan will lead the creation of a security environment in cyberspace with "no weak links" in the region. This will also contribute to ensuring the safety of the daily lives of Japanese nationals residing overseas and the business activities of Japanese companies that depend on critical infrastructure in the partner countries.

With regard to capacity-building support, Japan will strategically and efficiently implement such support in an "All-Japan" manner, through multilayered cooperation with diverse stakeholders, including its ally and like-minded countries, international organizations, industry, and academia. In doing so, with regard to the Indo-Pacific region, including ASEAN, and in light of the region's geopolitical importance, Japan will deepen cooperation in cyber diplomacy and national security by strengthening capacity-building support through the utilization of the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), as well as through cooperation with its ally and like-minded countries and international organizations.

In addition to human resource development and cyber exercises, Japan will provide capacity-building support in fields such as the understanding and practice of international law applicable to cyber activities, policy formulation, and advanced technologies that will shape the next generation of cyberspace. Furthermore, through international conferences and other forums, Japan will promote the branding of its cybersecurity, thereby contributing to the development of an ecosystem that supports Japan's cyber response capabilities, while also supporting the overseas expansion of cybersecurity-related businesses.

(iii) Promotion of international rule-making

International law, including the Charter of the United Nations, applies in cyberspace. Internationally wrongful acts by a state in cyberspace entail the responsibility of that state, and the victimized state may, in certain cases, take proportionate countermeasures and

other lawful responses against the state responsible. Furthermore, even when it cannot be confirmed that a preceding malicious cyber activity is attributable to a state, it is permitted to take certain measures by invoking necessity under international law, if certain conditions are met.

Under this approach, toward ensuring “a free, fair and secure cyberspace,” government officials at various levels will serve as the “face” of Japan in international forums, disseminating Japan’s fundamental principles. Japan will coordinate with its ally and like-minded countries and play an active role in promoting the rule of law in cyberspace and in international rule-making in line with Japan’s fundamental principles. Japan will also actively participate in and contribute to discussions on international law and international rule-making related to cyber activities, mindful that Active Cyber Defense, including remote access and neutralization measures, constitutes state practice that may influence the formation of international legal norms.

International rule-making is progressing within frameworks such as the United Nations and the G7, as well as through other multilateral frameworks among allies and like-minded countries. Japan will make every effort to ensure that international rule-making and their operation in cyberspace contribute to the peace and stability of the international community and to Japan’s national security. Japan will counter attempts to hinder the sound development of cyberspace in cooperation with all stakeholders, including its ally, like-minded countries and private organizations.

Furthermore, taking into account the impact of advanced technologies such as AI and quantum technologies on cyberspace, Japan will promptly advance efforts on international rule-making from the perspective of defense and deterrence against cyber threats.

2. Enhancement of Cybersecurity and Resilience Across Society by Broad Participation

Any stakeholder participating in cyberspace may become a target of cyberattacks. Furthermore, in the event of a cyberattack, there is a risk that damage may extend to third parties through the leakage of third-party information assets held by the affected entity, or through the use of its devices or systems as footholds for further attacks.

In addition, from the perspective of economic security, there is a growing need to ensure the appropriate handling of critical important data and so on, including processing and storage, that could undermine the safety of the nation and its people if leaked externally.

Under these circumstances, each stakeholder, on the premise that it may itself become a target of attack, has a responsibility to implement appropriate measures, taking into account its own capabilities and the risks it poses to society, to prevent and reduce cyber damage not only to itself but also to society as a whole. As such measures are also expected to generate synergistic effects with the defense against and deterrence of cyberattacks that pose serious threats to national security, the government will play a proactive role, including by implementing comprehensive measures, to promote positive initiatives by all stakeholders.

Today, government agencies and related agencies, as well as critical infrastructure operators, are targets of organized and refined state-sponsored cyberattacks. If damage were to occur, it could have a significant impact on the people's daily lives, socioeconomic, and ultimately national security. These organizations, therefore, bear substantial responsibility for ensuring cybersecurity in order to fulfill their social responsibilities.

Moreover, in today's environment where a wide range of products and services, companies, and organizations are interconnected and linked to cyberspace, the roles and responsibilities of vendors that manufacture, develop, and provide products and services are becoming increasingly significant. If SMEs suffer damage from cyberattacks, there is a risk that such damage may have a substantial impact on companies and other entities linked through supply chains. Accordingly, they should aim to enhance their level of response measures, while also considering collaboration with client organizations and the utilization of public support. Through these efforts, all organizations must secure cybersecurity and enhance resilience under the concept of "mission assurance[32]," whereby each organization, based on its capabilities and the risks it would pose to society if it were to suffer a cyberattack, strives to ensure the reliability of the entire supply chain, from the operations it must perform to the products and services it provides to the end user.

Furthermore, if each citizen is able to undertake basic efforts and measures, this is expected not only to reduce individual harm but also to contribute to the enhancement of cybersecurity and resilience across society as a whole. To that end, it is important for diverse

[32] All organizations, including private enterprises, critical infrastructure operators, and government agencies, should regard the operations and services they are required to perform as "missions" and secure the capabilities and assets necessary to reliably carry out those missions. This concept entails that cybersecurity initiatives should not be treated as ends in themselves; rather, the management and executives of each organization should identify the operations and services that constitute their "missions" and fulfill their responsibility for the secure and sustainable provision of those missions.

stakeholders from industry, academia, government, and the private sector to cooperate and, under appropriate role sharing, engage in awareness-raising activities and information dissemination in order to increase opportunities for individuals to acquire appropriate knowledge and translate it into action.

Through the synergistic effects of measures undertaken by a wide range of stakeholders, necessary investments, initiatives such as rule-making and standardization, and active defense and deterrence measures using diverse means, including remote access and neutralization measures, Japan aims to further enhance the level of cybersecurity and resilience across society as a whole. At the same time, Japan will simultaneously promote society-wide digitalization and the assurance of cybersecurity.

(1) Strengthening cybersecurity measures at government agencies and related agencies

Government agencies and related agencies should recognize that they are targets of sophisticated and advanced cyberattacks and that ensuring cybersecurity and resilience of their systems is important from the stand point of Japan's national security. Under this recognition, these bodies aim to serve as role models for other stakeholders by enhancing their cybersecurity measures, ensuring effectiveness including through audits and continuous reviews. Furthermore, they will strengthen and advance monitoring frameworks for their own systems.

Furthermore, while the government is promoting digital reform aimed at realizing "human-friendly digitalization that leaves no one behind," cybersecurity is indispensable to allow citizens to enjoy the benefits of a digital society. Accordingly, information systems of government agencies and related agencies should be developed, with due consideration given to cybersecurity from the construction stage.

Additionally, the government is set to further enhance development of human resources, with a view to build staff including those who are responsible for strengthening analytical capabilities and promoting public–private collaboration.

(i) Improving the level of cybersecurity and regularly reviewing common cybersecurity standards

Based on the Common Standards Group for Cybersecurity Measures for Government Agencies and Related Agencies (hereinafter referred to as the common cybersecurity standards [33]), each government agency and related agency must, under its own responsibility, conduct risk analysis and evaluation taking into account the characteristics of its operations, the information it handles, and the information systems it possesses; determine the priorities of measures to be implemented and the required level of cybersecurity measures; and implement appropriate measures. At the same time, the

[33] This constitutes a unified framework for improving the information security level of national administrative agencies and incorporated administrative agencies and sets forth the information security baseline for such agencies as well as the measures required to ensure a higher level of information security.

government is to improve response measures across government agencies and related agencies by regularly reviewing common cybersecurity standards, required for compliance by all government agencies and related agencies, as well as the Information System Security Management and Assessment Program (ISMAP[34]) for government information systems, and through advancing new initiatives in line with the changing environment and social conditions.

a. Continuous review of common cybersecurity standards and audits with a clear focus on leveraging monitoring results

The government will respond to constantly emerging cyber threats and risks by conducting ongoing reviews of the common cybersecurity standards. In doing so, taking into account that the scope of application of the common cybersecurity standards is broad and that information systems are highly diverse, revisions will be advanced to better reflect actual conditions. For example, in addition to presenting the baseline measures to be implemented, the common cybersecurity standards will also set forth higher-level measures to serve as reference points when government each agency and related agency consider more advanced cybersecurity measures, thereby enabling each organization to flexibly implement high-level cybersecurity measures.

In addition, each government agency and related agency, including external agencies, regional branches, and facilities, under its own responsibility, to implement information security measures in accordance with the common cybersecurity standards. To ensure that such measures are reliably implemented, including in the management of information systems, the National Cybersecurity Office will conduct focused audits making use of monitoring results and other information, and, through bodies such as the "Cybersecurity Strategy Promotion Council[35]" established under the Headquarters, will work to ensure thorough implementation and improvement of measures across ministries and agencies.

b. Continuous review of ISMAP

With the advancement of cloud services, the information handled in cloud environments by government agencies and related agencies has diversified in both type and volume. In response, the government will review the system to rationalize the required cybersecurity levels according to the type of information handled and to enable the flexible adoption of the latest cybersecurity measures.

Furthermore, in light of the continued evolution of cloud services, the government will conduct ongoing reviews of the system, taking into account the operational status of

[34] ISMAP is an abbreviation for Information System Security Management and Assessment Program (commonly referred to as "ISMAP"). The system was put into operation in FY2020 as a cybersecurity assessment framework for cloud services used in government information systems.

[35] This council is convened, with the Minister of State for Cybersecurity serving as Chairperson and bureau-level executives of each ministry as members, to enable relevant administrative organs to exchange information and views, promote coordination, and examine and advance comprehensive measures for enhancing Japan's cyber response capabilities and ensuring cybersecurity.

ISMAP, overseas initiatives, and revisions to international standards.

c. Review of the handling of highly confidential information in government agencies and related agencies

With the increasing sophistication of cloud technologies in recent years, the expanded use of such technologies by government agencies and related agencies in Japan is an inevitable trend, given their advantages in availability, scalability, and redundancy.

On the other hand, with regard to the handling of highly confidential information by government agencies and related agencies, it is necessary to appropriately ensure confidentiality, integrity, and availability in a manner that remains under Japan's control. Accordingly, taking into account the status of cloud technology utilization by government agencies and related agencies in other countries, studies will be conducted on the appropriate use of cloud technologies, including the scope of their implementation, premised on information security and the safeguarding of classified information. A policy direction will be presented around the summer of 2026, and a certain conclusion will be reached by the end of that fiscal year.

d. Reducing supply chain risks in IT procurement by government agencies and related agencies

In IT procurement and related activities by government agencies and related agencies, the equipment and services procured are expected to change in response to evolving circumstances and technological advances. At the same time, against the backdrop of the expansion and increasing complexity of supply chains, concerns have arisen regarding the latent emergence of risks. To sufficiently reduce supply chain risks[36] amid such changing environmental conditions, the government will ensure effectiveness by continuously reviewing relevant frameworks and systems, including the establishment of technical verification methods, while maintaining consistency with related systems.

(ii) Further strengthening and advancing government agencies and related agencies monitoring systems and incident response capabilities

Under the Basic Act on Cybersecurity as amended in 2025 (hereinafter referred to as the "Amended Basic Act"), as part of the evaluation of the status of cybersecurity assurance at government agencies and related agencies newly added to the functions of the Headquarters, existing initiatives, such as the GSOC's cross-government monitoring of malicious communications will be strengthened and advanced in cooperation with public-sector organizations (NICT and IPA).

The National Cybersecurity Office will advance enhancements to GSOC sensors to expand detection capabilities and conduct studies to further collect and aggregate

[36] Risks to the reliability and stability of cyberspace, including the risk that malicious functions may be embedded in products during the supply chain process, as well as the risk of disruptions to the supply of devices and services due to political and economic conditions.

information necessary for monitoring government agencies and related agencies. In addition, GSOC functions will be continuously adapted to support cloud monitoring. Furthermore, as part of a multi-layered defense for government agencies and related agencies, CYXROSS sensors[37] will be deployed across terminals of government agencies and related agencies, including all ministries and bodies, with effective monitoring targets determined as appropriate and used to conduct monitoring and analysis[38]. In addition, from the perspective of ensuring appropriate responses at the time of incidents, the National Cybersecurity Office will endeavor to grasp asset information and, with respect to information assets of each government agencies and related agencies that are exposed to the Internet, will continue initiatives such as vulnerability assessments and timely remediation, thereby strengthening vulnerability response at government agencies and related agencies. To ensure the effectiveness of these initiatives, each government agencies and related agencies will, in close coordination with the National Cybersecurity Office, provide information necessary for monitoring and work to enhance response measure levels.

Based on the above initiatives, the government will strengthen the analysis of information on cyberattacks targeting government agencies and related agencies. In addition, it will generate information that contributes to ensuring cybersecurity at each government agencies and related agencies, as well as information on unknown cyber threats. To this end, studies will be conducted on methods for more efficient and effective analysis of the increasing volume of logs and monitoring information collected and aggregated as a result of the expansion of cloud monitoring and the introduction of CYXROSS. In particular, as sophisticated attacks using AI are already being conducted, the defensive side will also continue to advance the utilization of AI. In addition, by deepening cross-organizational threat hunting and correlation analysis of incidents across each government agencies and related agencies, detection capabilities against attacks that are difficult to identify will be expanded, and digital forensic capabilities will be enhanced to address sophisticated and advanced cyberattacks.

Moreover, in order to prevent the spread of damage caused by such cyberattacks, insights obtained through analysis will be proactively provided. For example, indicators of compromise (IoC) information will continue to be shared within government agencies and related agencies, and will also be provided through the framework of the New Council.

(iii) Building and operating robust government information systems

In order to balance improvements in convenience from the perspective of citizens with the need to ensure cybersecurity, the Digital Agency has formulated the “Basic Policy on Cybersecurity for the Management of Government Information Systems” (attached to the

[37] A sensor developed by NICT that enables verification of safety and transparency.
[38] Furthermore, these efforts will contribute to strengthening Japan’s security technologies and development capabilities by sharing insights obtained through the analysis of primary information collected by CYXROSS, with the private sector (see III.3.(2)).

“Basic Policy for Development and Management of Information Systems” (decided by the Minister for Digital Transformation on December 24, 2021)) for government agencies and related agencies. Based on this policy, and taking into account the increasing severity of cyber threats, a promotion of the further implementation of cybersecurity measures across government information systems throughout their lifecycle, from planning through operation, by formulating and continuously reviewing the Standard Guidelines for the Promotion of a Digital Society and related cybersecurity documents will be continued.

In addition, the Digital Agency will ensure the resilience of, and strengthen the cybersecurity of, critical government information systems, including infrastructure systems for services to citizens that are developed and operated by the Agency, as well as systems that are commonly used by various ministries and agencies, by implementing measures such as enhancing incident response capabilities through monitoring and conducting audits and vulnerability assessments. Furthermore, the Agency will promote enhanced cybersecurity for government agencies and related entities by developing systems for monitoring operational status (COSMOS [39]) and mechanisms for continuously identifying and addressing risks through the management of information assets and vulnerabilities (CRSA[40]), as well as by promoting wider adoption among government organizations of Government Cloud and Government Solution Services (GSS) , which are securely designed.

Furthermore, each government agencies and related agencies will conduct risk analysis and evaluation based on the characteristics of its own operations and information systems, while taking into account the common cybersecurity standards and the Standard Guidelines for the Promotion of Digital Society. They will thoroughly implement the concept of ensuring cybersecurity consistently from planning through operation (Security by Design) in order to build information systems with appropriate levels of cybersecurity. At the same time, they will promote appropriate operation through the accurate management of information assets and vulnerabilities, as well as by ensuring early recovery in the event of an incident.

(iv) Development and retention of cybersecurity personnel and strengthening of organizational structures in government agencies and related agencies

In order to respond cyber threats appropriately, it is necessary to enhance the development of human resources such as strengthening analytical capabilities and promoting public–private collaboration. For this purpose, based on the concept of the cybersecurity human resources framework, the government will clarify the definitions of cybersecurity personnel required in each organization, formulate and implement training measures such as advanced training and exercises that incorporate cybersecurity

[39] COSMOS is an abbreviation for Comprehensive Operation and Monitoring System (commonly referred to as “COSMOS”).
[40] CRSA is an abbreviation for Continuous Risk Scoring and Action (commonly referred to as “CRSA”).

literacy, and link the framework to the efficient and effective operation of government mechanisms concerning personnel exchanges with the private sector and the utilization of highly specialized external experts.

In particular, it is essential to develop human resources with advanced response capabilities who well understand attacker's methods, able to detect threats lurking within networks at an early stage, and can respond swiftly and appropriately. The government will promote the development of core response personnel in government agencies and related agencies by establishing a new, realistic, large-scale exercise environment that enables regular training from an attacker's perspective.

Furthermore, formulate a "Digital Talent Acquisition and Development Plan." at each ministry and under the control tower function led by Deputy Director-General for Cybersecurity and Information Technology Management, the ministries and agencies concerned will steadily implement measures including the establishment of necessary organizational frameworks; the proactive recruitment of successful candidates from the "Digital" category of the Comprehensive Service Examination and the "Digital, Electrical, and Electronic" category of the General Service Examination; the implementation of training and exercises; the promotion of qualification acquisition; the ensuring of appropriate treatment; and the flexible management of terms of office in accordance with the nature of operations in each ministry and to strengthen the action, each plan will be followed-up every fiscal year.

In addition, the government will promote the development of an environment that can enhance their skills for talented people by moving between government agencies and private-sector companies, including through consideration of appropriate forms of cooperation with relevant businesses.

(2) Strengthening cybersecurity measures for critical infrastructure operators and local governments, etc.

Critical infrastructure[41], which serves as the foundation for people's daily lives and economic activities, must be protected through close public–private collaboration to ensure the safe and continuous provision of services.

Furthermore, in light of the fact that local governments hold large amounts of sensitive information, the government will provide necessary support to ensure that appropriate cybersecurity measures are implemented by local governments as well, while taking into account the division of roles between the national and local levels.

In addition, for universities and inter-university research institutes (hereinafter referred to as "universities and related institutions"), where the application of uniform measures across the entire organization is difficult, it is important to maintain and enhance cybersecurity levels autonomously through the leadership of the heads of these

[41]Services provided by businesses that form the foundation of daily lives of people and economic activities, for which viable alternatives are difficult to secure, whose suspension or deterioration would pose a significant risk to daily lives of people or economic activities, and that belong to critical infrastructure sectors.

corporations. To this end, the government will support autonomous initiatives by universities and related institutions.

(i) Strengthening cybersecurity measures for critical infrastructure operators

Regarding cybersecurity measures for critical infrastructure operators[42], the public and private sectors are working in close collaboration under the “Action Plan for Cybersecurity of Critical Infrastructure” (decided by the Cybersecurity Strategic Headquarters on June 27, 2025; hereinafter referred to as the “Action Plan”). However, as the risks of cyberattacks targeting critical infrastructure have become apparent, there is a need to further strengthen these measures.

To this end, through the new system established by the Amended Basic Act, Japan will strive to ensure the thorough implementation of basic measures that should be taken across various sectors and operators, while raising the cybersecurity level of critical infrastructure as a whole by reviewing the Action Plan in light of changes in the environment surrounding the critical infrastructure sector.

a. Formulation of common cybersecurity standards for critical infrastructure and initiatives based on them

Currently, standards and guidelines are established in each critical infrastructure sector based on the Guideline for Establishing Safety Principles for Ensuring Cyber Security of Critical Infrastructure, etc., under the Action Plan. On the other hand, there are no specific and unified standards that enable the evaluation and improvement of initiatives in each sector, and cybersecurity measures and levels vary across sectors and operators. To respond to cyberattacks that are becoming more sophisticated and advanced year by year, it is necessary to ensure the thorough implementation of baseline measures across sectors and operators by critical infrastructure operators.

To this end, pursuant to the Amended Basic Act, the state will establish specific and unified standards (hereinafter referred to as the “common cybersecurity standards for critical infrastructure”) regarding the measures to be implemented by national administrative agencies to ensure the cybersecurity of critical infrastructure operators.

Japan aims to raise the cybersecurity level of the critical infrastructure sector as a whole by establishing a PDCA cycle through the common cybersecurity standards for critical infrastructure. Specifically, this will involve: specialized investigations by the National Cybersecurity Office into the status of initiatives undertaken by critical infrastructure operators in each sector, conducted through the relevant ministries; the compilation by those ministries of the status of implementation of measures based on the results of those investigations; and evaluations conducted by the Headquarters. These steps will lead to improvements in both the measures implemented by the

[42] Critical social infrastructure operators as defined in Article 12, paragraph (2), item (iii) of the Basic Act, organizations formed by such operators, and local governments.

ministries responsible for each sector and the initiatives undertaken by critical infrastructure operators in each sector.

Regarding public–private information sharing, a more effective framework will be established by organizing the approach to information sharing, including the scope of information sharing and the flow of communication, based on the common cybersecurity standards for critical infrastructure and related systems.

The formulation of the common cybersecurity standards for critical infrastructure will be conducted in FY2026, considering existing systems and international, technological, and threat trends. Furthermore, the Action Plan will be reviewed in FY2026 based on these standards and the systems applicable to essential infrastructure service providers. In addition, further reviews [43] will be conducted in response to changes in the cybersecurity environment surrounding critical infrastructure.

b. Nature of the protection scope for critical infrastructure

The target sectors and operators for “critical infrastructure operators” under the Basic Act and for “essential infrastructure service providers” are determined in accordance with the intent of the law, and differences exist between them.

In light of the increasing importance of ensuring cybersecurity for essential infrastructure service providers, such as the requirement for incident reporting under the Cyber Response Capability Strengthening Act, Japan will consider reviewing the nature of the protection scope for critical infrastructure. For example, this may include newly positioning sectors and operators among essential infrastructure that are not currently included in critical infrastructure as targets for critical infrastructure protection, while taking into account their respective characteristics.

In this review, Japan will strive to ensure the thorough implementation of basic measures to be taken across sectors and operators based on the common cybersecurity standards for critical infrastructure, including cybersecurity measures that serve as a prerequisite for notifications and incident reporting under systems targeting essential infrastructure service providers, so as to ensure that the relevant operators undertake more effective initiatives.

c. Initiatives in individual sectors

Among critical infrastructure sectors, it is necessary to promote sector-specific initiatives, particularly in sectors that have suffered especially serious damage but have not made sufficient progress, as well as sectors that have a major impact on people’s daily lives and economic activities.

For example, in the medical sector, incidents have occurred in which cyberattacks have significantly disrupted clinical services over extended periods due to insufficient cybersecurity measures at external contractors or inadequate oversight by contracting

[43] Reviews conducted pursuant to “VI. Evaluation and Verification” and “VII. Review of This Action Plan” of the Action Plan.

entities. To minimize the impact of incidents on clinical services, the government will promote awareness of the “Guidelines for the Safety Management of Medical Information Systems,” provide support for initial response toward recovery, and continue to support the management of external network connection points (hereinafter referred to as “external connection points”) that may serve as intrusion routes for attacks.

Furthermore, based on the results of management status surveys of external connection points, the government will provide support for compliance with the aforementioned guidelines, including the optimization of external connection points. In addition, for medical devices that form part of the external connection points in medical institutions, the government will formulate guidelines for marketing authorization holders and provide support to strengthen cybersecurity.

(ii) Strengthening cybersecurity measures for local governments

Furthermore, in light of the fact that local governments hold large amounts of sensitive information, including personal information, and provide essential services closely related to people’s daily lives and local economic activities, the government will provide necessary support to ensure that cybersecurity measures are appropriately implemented by local governments, while taking into account the division of roles between the national and local levels.

Based on the Local Autonomy Act (Act No. 67 of 1947), as amended in 2024, local governments will be obligated to formulate a policy for ensuring cybersecurity starting from FY2026. To ensure the effectiveness of measures implemented under the policy, the government will proceed with further efforts to strengthen the cybersecurity foundations of local governments, taking into account the newly formulated common cybersecurity standards for critical infrastructure[44].

Specifically, the state will implement initiatives to further enhance safety, including: providing financial support for the smooth upgrading of local government information security clouds; supporting[45] the securing and development of digital human resources; providing training programs, such as the Cyber Defense Exercise with Recurrence (CYDER), necessary for building personnel frameworks; promoting the use of the Local Government CSIRT Council operated by the Japan Local Government Data Systems Organization (J-LIS); and establishing a system to diagnose vulnerabilities inherent in local government information systems in order to strengthen their vulnerability response capabilities. Furthermore, to enable each local government to conduct information security audits, the state will take appropriate financial measures and strengthen efforts to secure the budgets and personnel necessary to implement cybersecurity measures.

[44] The common standards set forth the criteria for measures to be implemented by national administrative agencies to ensure cybersecurity at critical infrastructure operators and the term “critical infrastructure operators” includes local governments.
[45] To enable prefectural governments to establish DX promotion frameworks in collaboration with municipalities, and within such frameworks, to secure pooled digital personnel to support municipalities, the government will take local fiscal measures to support prefectural governments in securing such personnel for municipal support. It will also provide hands-on support and other assistance to enable the planned securing and development of digital personnel.

In addition, Japan will consider establishing a new mechanism that allows all local governments to reliably implement cybersecurity measures, including supply chain risk measures.

Furthermore, the government will continue to support the initiatives of local governments to ensure that measures based on the “Guidelines Regarding Information Security Policy in Local Governments” are appropriately implemented.

With regard to My Number, which is closely linked to people’s daily lives and personal information, the government will continue to strengthen measures while maintaining an appropriate balance between convenience and cybersecurity, thereby promoting its safe and secure use.

(iii) Strengthening cybersecurity measures for universities and related institutions

Universities and related institutions, are composed of diverse members and possess a wide variety of information assets. Moreover, rooted in the spirit of academic freedom, they have a culture in which the independence of each constituent entity is respected, making it difficult to apply uniform information security measures across the entire organization. Under these circumstances, for universities and related institutions, to fulfill their roles in education, research, and social contribution while ensuring a safe and secure education and research environment, it is important to deepen further recognition that cybersecurity measures have become a major management issue. Taking into account their organizational characteristics, the heads of these corporations must exercise leadership to continuously maintain and enhance cybersecurity levels in response to changes in the situation.

Therefore, to support autonomous initiatives by universities and related institutions, the government will provide support such as advice and information sharing regarding cybersecurity measures and structure development, organizational arrangements, as well as the conduct of training and exercises and the provision of advice when incidents occur. Furthermore, in order to ensure research security for universities and related institutions, that implement research and development programs for which the prevention of technology leakage is particularly necessary from the perspective of economic security, the government will provide support from a cybersecurity perspective as needed to ensure research security.

(3) Ensuring cybersecurity and resilience across the entire supply chain, including vendors and SMEs

Traditionally, cybersecurity has been regarded as a matter to be ensured by each company. However, with the widespread adoption of digital transformation (DX) across society, cyberattacks targeting a specific company can now affect the entire supply chain, including its contractors and business partners. Against this backdrop, and in light of

international trends such as the principles of Secure by Design and Secure by Default, as well as the introduction of new provisions[46] in the Amended Basic Act defining the responsibilities of the suppliers of information systems, etc., cybersecurity across the entire supply chain has become an essential requirement. Accordingly, efforts will be undertaken to ensure cybersecurity and resilience throughout the supply chain.

In doing so, it is also important to identify challenges in existing systems that could become impediments, and to work toward their resolution. Accordingly, the National Cybersecurity Office will work in coordination with relevant ministries and agencies to promote initiatives such as the dissemination of the Secure by Design and Secure by Default principles and the enhancement of security governance. These initiatives will include identifying practical cybersecurity challenges in operational and field settings, comprehensively coordinating with relevant ministries, agencies, and private-sector companies toward their resolution, engaging in rule-making from a society-wide perspective, and awareness-raising activities and understanding of laws and regulations related to cybersecurity.

(i) Promoting responsible cybersecurity practices among vendors based on secure-by-design principles ,etc.

To promote the secure design, development and maintenance of information systems, the responsibilities that the suppliers of information systems, etc. should fulfil in relation to users will be clearly defined. Additionally, systems will be developed to ensure that the responsibilities of suppliers are embedded throughout society, such that it becomes a matter of course for users to access secure services and products and to easily ensure their own cybersecurity.

With regard to the “JC-STAR” scheme, which certifies IoT products that meet a certain level of cybersecurity, further institutional development will be advanced. In combination with various measures such as guidelines and subsidies, its use will be promoted across society, including government agencies, local governments, critical infrastructure operators, and industry, while at the same time promoting interoperability with similar schemes in other countries. Similarly, the use of tools that enhance software transparency, including SBOM (software bill of materials), as well as the practice of secure software development, will be promoted across society. At the same time, Japan will work in a leading role to advance efforts toward institutional harmonization with other countries.

(ii) Ensuring cybersecurity and resilience throughout the supply chain

To ensure cybersecurity and resilience across the entire supply chain, it is necessary to incorporate cybersecurity perspectives into corporate management, treating it not merely as a system management issue but as a matter of comprehensive risk

[46] Article 7, Paragraph (2) of the amended Basic Act

management. Accordingly, the government will more strongly promote changes in management awareness and corporate behavior. It will work to develop an environment that enables companies to procure secure products and appropriately select business partners. At the same time, initiatives will be promoted to create incentives for cybersecurity measures, including the enhancement of transparency for stakeholders such as investors who place importance on sustainability.

Specifically, during FY2025, illustrative cases will be added to guidelines that clarify the applicability of relevant laws and regulations concerning support for, and requests to, suppliers by client companies with regard to cybersecurity measures, and these guidelines will be disseminated to relevant industries and stakeholders. In FY2026, a scheme to visualize and verify the levels of cybersecurity measures that companies should adopt in accordance with supply chain risks will be launched, with the aim of promoting its adoption in collaboration with industry associations, including those in critical infrastructure sectors. Furthermore, all available measures will be mobilized to strengthen cybersecurity across the entire supply chain, including the expansion of existing initiatives such as industry-focused human resource development programs and support for initial responses to cyberattacks.

In addition, the use of the “Cyber-Physical Security Framework[47]” will be promoted in areas such as the construction of cross-industry data platforms and system integration, as well as in the architectural design of social and industrial structures. By continuously updating the framework while monitoring revisions to relevant international standards, it will effectively serve as a foundation that enables all stakeholders to freely form interconnections and linkages, thereby creating new value.

Furthermore, guidelines will be developed to address cybersecurity-related challenges associated with advanced technologies such as AI, robotics, and quantum technologies that are expected to see rapid adoption in the future, particularly in sectors with strong domestic investment or where enhanced autonomy is required from the perspective of economic security. At the same time, these guidelines will be linked with government measures, including support for investment and technology development, to establish mechanisms that ensure their effective implementation.

From the perspective of ensuring cybersecurity and enhancing autonomy for digital infrastructure that forms the foundation of a digital society, efforts will be made. For example, through collaboration between the public and private sectors and in cooperation with international partners efforts will be promoted to secure, protect, and ensure the safety, reliability, and redundancy of critical infrastructure such as international submarine cables, on which most communications between Japan and

[47] The Cyber-Physical Security Framework is a set of guidelines that set out the cybersecurity measures required in “Society 5.0” to address new risks arising from: (i) the expansion of data circulation and linkage in cyberspace; (ii) the integration of physical and cyber spaces; and (iii) the increasing complexity of intercompany supply chains, which can lead to the diffusion of the sources of cyberattacks and amplified impacts on physical space.

overseas depend, while at the same time establishing autonomous capabilities for their production, installation, and maintenance.

(iii) Strengthening measures for individual private companies, including SMEs

Cybersecurity measures at SMEs and other private-sector companies are essential to ensure cybersecurity and resilience across the entire supply chain. Meanwhile, SMEs and similar companies continue to face challenges such as insufficient awareness of the need for cybersecurity measures and difficulties in securing adequate resources, including personnel and budgets. Therefore, it is necessary to further strengthen initiatives that combine “self-help,” “mutual help,” and “public help,” implemented through collaboration among the government, industry associations, and support organizations.

As an initiative to encourage “self-help” among SMEs and similar companies, efforts will include the development of guidelines and model regulations to promote the use of a system that visualizes and verifies the level of cybersecurity measures each company should adopt in accordance with supply chain risks, as well as the dissemination of relatable examples and preventive measures that SMEs can easily understand and apply.

As an initiative to encourage “mutual help” among supply chain stakeholders, efforts will include the establishment and promotion of a system that visualizes and verifies the level of cybersecurity measures each company should adopt in accordance with supply chain risks; the identification and development of leading entities in regions where local and voluntary cybersecurity awareness activities are not yet active; the promotion of collaboration with locally rooted organizations such as regional financial institutions and professional service providers; the strengthening of outreach and dissemination activities through industry-led consortia established to enhance cybersecurity across the entire supply chain, including SMEs; and the facilitation of the dissemination and sharing of cyber-related information.

For SMEs that still face difficulties in adequately addressing cybersecurity, ”public help” will be promoted through efforts, including reviews that will be conducted to improve the use of the Cybersecurity Supporters Service, and the establishment and facilitation of mechanisms that enable SMEs to easily identify and request support from external cybersecurity experts. In addition, the introduction of a “collective defense” framework will be promoted, under which telemetry information[48] from SMEs and other companies belonging to the supply chains of essential infrastructure service providers will be collected, integrated, and analyzed, and useful information, such as cyberattack detection data, will be fed back to strengthen their cybersecurity measures. Through these initiatives, cybersecurity measures of SMEs and other companies that underpin the entire supply chain will be supported.

[48] Telemetry information refers to data collected in the form of system operational status or event logs (including records of unauthorized access) and transmitted to a remote location for monitoring and analysis.

(4) Improving cybersecurity by full participation

Amid increasing cyberattack risks targeting all actors, including individuals and SMEs, it is expected that, if each citizen deepens their awareness and understanding of cybersecurity and voluntarily implements basic measures and practices on a routine basis, this will not only reduce individual harm but also create synergistic effect with cybersecurity measures and responses undertaken by the government, companies, and other stakeholders, thereby contributing to the enhancement of cybersecurity and resilience across society as a whole.

In particular, at the individual level, cyber threats are increasingly affecting senior citizens and younger generations, while at the organizational level, smaller companies and organizations face challenges such as insufficient resources for implementing cybersecurity measures. While various organizations, including the national and local governments and private-sector entities, have engaged in awareness-raising activities, it is challenging to ensure that such information is effectively disseminate. It is still necessary to focus on senior citizens, younger generations, and SMEs as key target groups and to provide effective awareness-raising activities and information provision tailored to their respective needs and circumstances, so that they can understand and practically implement concrete cybersecurity measures.

To date, the government has supported mechanisms for collaboration and coordination among stakeholders by disseminating information through websites and social media, holding training sessions, developing content such as handbooks and teaching materials, and promoting initiatives during Cybersecurity Month. The government will continue to play this role while appropriately updating content to reflect changing environments and diverse needs, and by expanding and strengthening collaboration with stakeholders to ensure that information reaches a wider citizen. In doing so, the government will also give due consideration to the dissemination of information on the increasingly severe situation surrounding cyberspace, with a view to promoting response measures and actions by a wide range of stakeholders.

Moreover, the importance of information education has been steadily increasing, and even at the elementary and secondary education levels, the use of digital learning infrastructure, such as 1 device for 1 student, has been advancing in tandem with the promotion of the GIGA School Program. In promoting the GIGA School Program, efforts are being made to enhance teachers' ICT instructional skills and to strengthen [49] information education, including information security, for students in line with the curriculum guidelines, with the aim of cultivating "information literacy" as a foundation for learning. In addition, taking into account the latest developments surrounding the Internet, efforts are being made regarding awareness-raising activities[50] and providing guidance to ensure that young people can use the Internet safely and appropriately.

[49] Information Ethics Education Portal Site (https://www.mext.go.jp/zyoukatsu/moral/index.html)
[50] Toward measures to address harmful environments surrounding youth (https://www.mext.go.jp/a_menu/sports/ikusei/taisaku/index.htm)

Furthermore, with regard to IoT devices that are widely used by the public, relevant entities will work together to ensure cybersecurity by providing users and vendors with warnings, guidance, and information[51] on misconfigurations and vulnerabilities, thereby enabling each party to implement appropriate response measures and promoting a unified approach to cybersecurity.

It is desirable for diverse stakeholders in industry, academia, the public and private sectors to actively collaborate and coordinate in conducting awareness-raising activities and information dissemination, so that their respective initiatives generate synergistic effects and appropriate knowledge and actions spread widely.

All stakeholders must collaborate in steadily advancing these initiatives, while continuously monitoring and evaluating their progress and effectiveness, and taking measures to improve them. In addition, the key target audiences, dissemination methods, and content should be reviewed and updated as necessary in response to changing circumstances.

(5) Ensuring safety and security in cyberspace through measures against cybercrime

In light of the fact that cyberspace is evolving to become a public space in which all stakeholders are involved, the government continues to push forward with the crackdown on criminals and criminal groups that exploit the anonymity of cyberspace, such as through crypto-assets and social media, as well as malicious business operators that provide criminal infrastructure hindering traceability, with the aim of ensuring a level of safety and security equivalent to that in physical space.

Furthermore, efforts will be strongly promoted to collect and organize information necessary for responding to major cyber incidents[52] and to conduct comprehensive and cross-case analyses will be promoted strongly. At the same time, investigative capabilities and technical expertise will be enhanced to effectively address crimes involving the malicious use of AI and other technologies, as well as crimes that exploit advanced information and communications technologies, such as ransomware.

The government will also prevent cyberspace from becoming criminal infrastructure through public- and private-sector collaboration, leveraging information on infrastructure and technologies that are at high risk of being exploited for criminal purposes, as identified through criminal investigations, and by engaging with relevant business operators. In addition, from the perspectives of information sharing and analysis, prevention of damage, and human resource education, the government will promote measures against cybercrime by utilizing industry–academia–government collaboration frameworks. To prevent damage from cybercrime by encouraging voluntary measures by each individual, the government will collaborate with relevant institutions and organizations, including

[51] For example, the NOTICE project (https://notice.go.jp/)
[52] This refers to major cyber incidents as defined in Article 5, Paragraph (4), Item (vi), c. of the Police Act (Act No. 162 of 1954).

cybercrime prevention volunteers, and advance public awareness and outreach activities.

For the purpose of dealing with crime where advanced information and communication technologies are used, the government will strengthen its digital forensics capabilities, enhancing the technological prowess to analyze the latest in digital devices or malicious software, and advancing comprehensive analysis for signs of threats in cyberspace and for unraveling those threats technologically.

In addition to these efforts, in order to appropriately address cyber incidents carried out across national borders, the government will promote necessary measures, such as cooperation with relevant businesses and international collaboration with foreign authorities, while drawing on the status of initiatives in other countries.

3. Formation of an Ecosystem for Human Resources and Technologies Supporting Japan's Cyber Response Capabilities

In order to give concrete form to defense and deterrence against increasingly severe cyber threats through diverse means, as well as to the enhancement of cybersecurity and resilience across society through the participation of a wide range of stakeholders, and to elevate Japan's cybersecurity level to one of the highest in the world, it is necessary for Japan to secure the human resources and technologies that underpin these efforts.

However, in Japan, a shortage of such human resources has long been pointed out. If cybersecurity personnel are not strategically developed and secured, there is concern that ensuring cybersecurity will become increasingly difficult due to persistent shortages of such personnel.

Moreover, Japan relies to a considerable extent on overseas sources for digital technologies and industries themselves, and the cybersecurity field is no exception. From a national security perspective, it is necessary to ensure autonomy by fostering domestic industries with a base in Japan and by enhancing technological and development capabilities.

Furthermore, while technological innovations such as AI and quantum technologies are expected to be utilized in the field of cybersecurity, concerns have also been raised regarding associated risks, including AI safety, the malicious use of AI in cyberattacks, and the deterioration of safety and potential compromise of existing public-key cryptography due to advances in quantum computing.

With regard to the development and securing of human resources, efforts will be made to broaden the talent base centered on the cybersecurity workforce framework, while also cultivating and securing highly skilled personnel with specialized knowledge and practical expertise.

In addition, for cybersecurity-related technologies that form the foundation of Japan's response capabilities, based on public-sector's needs in cyber domain, promote the development of its cybersecurity industry by expanding the implementation of research and development, development support, and demonstration projects, as well as by utilizing technical information generated through these efforts and supporting startups, etc.

With regard to advanced technologies such as AI and quantum technologies, Japan must take proactive and forward-looking actions and measures. The government will actively promote the development of the necessary enabling environments to react the benefits and risks these technologies cause to the cybersecurity field.

To promote necessary investments and build an ecosystem of human resources and technologies that support cyberspace through collaboration among industry, academia, and government, thereby establishing and maintaining a foundation for securing the personnel and technologies that underpin Japan's cyber response capabilities, reducing national security risks by avoiding excessive reliance on overseas sources in the cybersecurity field, and building a framework capable of responding to transformations in cybersecurity driven by emerging technological innovations.

(1) Efficient and effective development and retention of cyber workforce

As digitalization of the economy and society advances, cyberattacks are becoming increasingly complex and sophisticated, making the securing and development of cybersecurity personnel across all sectors an urgent priority. Therefore, centered on the cybersecurity workforce framework, efficient and effective personnel development will be promoted by organically linking various measures.

(i) Cybersecurity workforce framework

To effectively promote the securing and development of personnel in the cybersecurity field, it is important to promptly establish the cybersecurity workforce framework that systematically organizes the knowledge, skills, and other requirements for diverse roles, and it should be utilized across various sectors of society. This will enable companies, government agencies, universities, and educational institutions to undertake more effective and systematic development and recruitment of cybersecurity personnel based on common understanding of the required skill sets and roles.

In establishing the framework, the government will aim to create an environment in which personnel can thrive both within Japan and internationally. To this end, the framework should be highly practical, based on Japan’s public- and private-sector response systems, while ensuring consistency with existing domestic and international frameworks and occupational classifications.

After framework is established, the government and the private sector will work together to create a system that provides an overall view of domestic talent trends and centrally and comprehensively visualizes the supply and demand of human resources, based on the personnel definitions set forth in the framework.

It will strengthen the linkage between education and training provided by various stakeholders and the framework. Specifically, mechanisms will be promoted to link outcomes such as passing qualification exams or completing practical exercises to the roles and levels defined in the framework, thereby enabling the visualization of participants’ skills; these mechanisms will also be utilized in the design of education and training curricula. The government will promote the development of appropriate evaluation systems and the proper placement of personnel, including through coordination with the government digital talent skills certification system based on the framework.

These initiatives will enable diverse personnel to demonstrate their abilities in areas where they are needed in society, and will facilitate the organic circulation of knowledge and experience gained across various settings through human resources, thereby contributing to the sustained strengthening of cybersecurity levels across society as a whole.

(ii) Further enhancement of education, exercises, and training for developing cybersecurity personnel

In Japan, insufficiency of cybersecurity personnel who has specialized knowledge and practical skills continues to be pointed out. Meanwhile, efforts in both the public and private sectors, such as qualification systems, training and exercises, and opportunities for reskilling, are progressing. It is important to accelerate this momentum and advance the securing and development of cybersecurity personnel in terms of both quality and quantity.

From elementary and secondary education through higher education, vocational training, workforce development, and the cultivation of highly specialized personnel, there is a need to establish a systematic and continuous learning environment. Opportunities will be created for the step-by-step acquisition of skills ranging from foundational literacy (information literacy) to advanced expertise, while strengthening industry, academia and government collaboration to ensure access to practical skills training and the latest knowledge.

Specifically, efforts will include strengthening mathematics, data science, and AI education, including cybersecurity, at universities and colleges of technology (KOSEN) through the “Approved Program for Mathematics, Data science and AI Smart Higher Education,” as well as promoting advanced technical education programs for young people, such as the “Security Camp.” For young engineers, support learning applied capabilities and practical skills by offer curriculum on cutting-edge security technologies and development. For critical infrastructure operators and related entities, practical exercises and exercise platforms that enhance response capabilities, such as “CYDER,” “CYROP[53],” and the “Core Human Resource Development Program,” will be promoted. At the same time, training opportunities and diverse learning environments will be systematically developed and expanded, enabling participants to utilize them in a step-by-step manner. For personnel without specialized cybersecurity skills, learning opportunities will be enhanced so that they can acquire the knowledge necessary to collaborate with cybersecurity experts both inside and outside their organizations, thus making them plus-security personnel[54]. In addition, with regard to the national qualification of Registered Information Security Specialist, efforts will be made to expand the number of certified professionals by promoting its utilization, including support for cybersecurity measures at SMEs, while reducing the burden associated with qualification renewal. Furthermore, Capture The Flag (CTF) exercises, which cultivate practical problem-solving skills and contribute to the early identification of next-generation talent as well as the fostering of international professional networks, will be utilized in human resource development, taking into account their effectiveness.

[53] NICT’s exercise platform, which enables the easy development and implementation of practical exercises tailored to specific fields.
[54] Plus-security personnel refers to management personnel promoting digital transformation, who, even if they do not necessarily possess specialized knowledge or operational experience in IT or cybersecurity, supplement their capabilities by acquiring, in a timely manner, the additional knowledge (“plus-security knowledge”) necessary to collaborate with internal and external cybersecurity experts.

By organically linking these diverse learning initiatives through the cybersecurity workforce framework, learning opportunities will be provided on a continuous basis, and the knowledge and skills gained will lead to career development and opportunities for professional engagement. While maintaining an overarching view of the various education and training systems, continuous improvements will be pursued.

(2) Formation of an ecosystem for emerging technologies and services

Although the cybersecurity market is on an expansionary trend, the supply capacity of Japanese businesses, the absolute number of top-level talent engaged in product development, and collaboration among industry, academia, and government cannot be said to be sufficient.

To enhance Japan's response capabilities in the cybersecurity field, it is necessary to form a virtuous ecosystem centered on domestically developed technologies and services that foster both technologies and human resources. This will involve stimulating research and development, demonstrations, and related activities for new technologies and services within Japan, without excessive reliance on overseas technologies or services, and improving analytical and development capabilities through their early social implementation.

To build such an ecosystem, and based on government needs, efforts will be advanced to implement and expand research and development, development support, and demonstrations of cybersecurity-related technologies that are indispensable for the collection and analysis of threat information and that form the foundation of Japan's response capabilities. This will include the utilization of technical information, including primary data, generated through these efforts, as well as the promotion of their proactive use by government agencies and related agencies through measures such as startup support. In addition, by leveraging data and exercise platforms held by organizations such as national research institutions, efforts will be made to develop young talent and specialized personnel across various industrial sectors, thereby enhancing analytical and development capabilities in both the public and private sectors, promoting early social implementation, and fostering domestic industry.

Regarding research and development, the government is promoting R&D of advanced and critical technologies, including those in cybersecurity fields, and the utilization of their results, leading to both civilian applications and public use, that are essential for Japan to secure a firm position in the international community. Including these initiatives, the government will continue to actively collaborate with companies, research institutions, and other stakeholders to advance technological development in the cybersecurity field, including fundamental research, as well as efforts toward social implementation and international standardization.

Regarding the utilization of technical information, for example, the government will strengthen the collection and analysis of cyber threat information by introducing CYXROSS,

a cyberattack detection system built using Japan's own sensors (software), into government agencies and related agencies. The technologies, information, and know-how obtained through these efforts will not be confined within government bodies. They will be broadly available to the private sector under appropriate information security measures, thereby advancing initiatives to strengthen the development foundation for domestic security technologies.

Furthermore, with regard to the development of the cybersecurity industry, government agencies and related agencies will create an environment that fosters the continuous emergence of promising cybersecurity products and services from Japan. This will include the trial use of products and services from promising startups, etc. by government agencies; the utilization of prize-based grant programs to identify promising technologies and businesses; the establishment of mechanisms to ensure the appropriate evaluation of cybersecurity service providers; and the promotion and consideration of measures to support the overseas expansion of Japanese cybersecurity product and service providers.

These efforts will be promoted, as necessary, through international collaboration, on the premise that Japan's international competitiveness is maintained and that no national security concerns arise.

(3) Responses and initiatives for advanced technologies

With the rapid advancement of AI technologies, including generative AI, Japan is facing new threats such as the increasing sophistication of cybercrimes, including unauthorized access and fraud. Furthermore, as the utilization and proliferation of AI are expected to expand further, attacks targeting AI are expected to intensify, emerging as new cybersecurity risks.

In addition, with the advancement of quantum computing technologies, there is a need to address a wide range of challenges, including concerns over the deterioration of safety and potential compromise of currently widely used public-key cryptography.

In tandem with promoting the technological development efforts in the cybersecurity field described above in (2), necessary measures will be advanced to ensure timely and appropriate responses to digital technological innovations, taking into account the impacts that advanced technologies may have on cybersecurity, national security, and related areas.

However, recognizing that new technological innovations with significant impacts on cybersecurity may emerge unpredictably in the future, necessary responses will be implemented flexibly, even for the technologies not specifically cited in this Strategy, by closely monitoring such developments.

(i) Response and initiatives accompanying the advancement and spread of AI technology

The advancement and adoption of AI technologies are significantly impacting the field

of cybersecurity. Specifically, three perspectives can be identified: ensuring security to protect AI itself (Security for AI), ensuring cybersecurity by using AI (AI for Security), and addressing cyberattacks that exploit AI.

From these perspectives, in order to maximize the benefits that AI brings to cybersecurity while minimizing its negative aspects, a comprehensive range of approaches will be promoted. These will include research and development; rule-making, such as the development of guidelines; social implementation; and human resource development, taking into account international trends, technological advancements, and trends in cyberattacks. In doing so, care will be taken to ensure that Japan does not fall behind advanced countries in its response to AI.

With regard to ensuring Security for AI including AI safety, efforts will continue to secure technological capabilities, develop guidelines, and promote international cooperation in order to flexibly address the various types of attacks targeting AI. Specifically, in collaboration with organizations such as the AI Safety Institute (AISI) and taking international trends into account, efforts will be promoted to develop, revise, and disseminate guidelines related to AI development and operation. In parallel, through efforts including collaboration with overseas institutions, research and development addressing attacks on AI and the advancement of trustworthy AI will be promoted as part of broader initiatives to ensure cybersecurity. Regarding the Hiroshima AI Process, launched by Japan as the G7 Chair in 2023, efforts will be promoted to ensure AI governance that will include cybersecurity, both within Japan and internationally.

Furthermore, government agencies and related agencies will promote the utilization of AI, particularly generative AI, based on guidelines for its procurement and use, while ensuring both effective utilization and appropriate risk management, and doing so in a manner that ensures the safety of AI, including the addressing of cybersecurity concerns.

With regard to leveraging “AI for Security”, in response to the increasing scale and sophistication of cyberattacks in both quality and quantity, and amid growing demands for the processing of vast amounts of data and advanced analysis, the government will, in collaboration with relevant stakeholders, promote efforts including the use of AI to detect cyberattack infrastructures, as well as to refine and accelerate the analysis of related information.

With regard to cyberattacks that exploit AI, efforts will be promoted through initiatives including research and development to prevent damage from cyberattacks that are expected to pose an even greater threat as AI advances.

At the same time, initiatives will also be promoted to identify and develop personnel who possess expertise in both AI and cybersecurity.

AI technologies and cybersecurity are also critical from a national security perspective; however, dependence on overseas sources is increasing. Therefore, initiatives related to AI in the cybersecurity field will be promoted, in close coordination with various efforts to advance Japan-based research and development and social implementation, to

secure AI development resources, and to implement supply chain risk measures, along with efforts related to national security and the development of Japan's industry in the AI field.

These AI-related initiatives will be promoted based on the Basic AI Plan formulated by the AI Strategy Headquarters, in accordance with the Act on Promotion of Research and Development, and Utilization of Artificial Intelligence-related Technology (Act No. 53 of 2025)

(ii) Response and initiatives accompanying the advancement of quantum technology

Regarding quantum computing technology, concerns have been raised that its advancement may lead to the deterioration of safety and potential compromise of currently widely used public-key cryptography. In this context, countries such as the United States and the European Union (EU) have announced their respective policies for transitioning to post-quantum cryptography (PQC), many of which aim for the transition by 2035. The safety and reliability of cyberspace are built on the foundation of cryptographic technologies used to ensure information confidentiality, prevent tampering, and enable authentication. From the perspective of international collaboration, delays in Japan's transition could give rise to concerns regarding cybersecurity and national security. To ensure Japan's cybersecurity, government agencies and related agencies aim for the transition to PQC by 2035, in principle[55]. Taking into account the current use of cryptographic and other technologies at government agencies and related agencies, a roadmap will be formulated in FY2026 under collaboration with relevant ministries and agencies to promote smooth nationwide transition.

Furthermore, the transition to PQC is not limited to government agencies and related agencies; it is also an issue that must be considered by critical infrastructure operators and private-sector entities. Accordingly, under the collaboration with relevant ministries and agencies, examinations of necessary measures will be advanced to support a smooth transition.

Taking into account the accelerating efforts toward the social implementation of Quantum Key Distribution (QKD) in foreign countries, Japan will also advance initiatives aimed at the social implementation of QKD around 2030. These initiatives will include the expansion and enhancement of testbeds, the development and validation of use cases and business models, and other measures to ensure robust cybersecurity and strengthen international competitiveness.

[55] However, it is necessary to assess the importance of information and the current use of cryptographic and other technologies, carefully consider how to proceed with the transition, and make appropriate decisions accordingly. For example, in cases involving particularly sensitive information or information expected to require very long-term protection, each information system will be appropriately examined, including the option of undertaking an earlier transition.

IV. Implementation Framework of the Strategy

In advancing Japan's cybersecurity policy based on this Strategy, a unified, government-wide implementation framework is required more than ever before. Based on the amended Basic Act, the Headquarters was reorganized into a new organization headed by the Prime Minister and composed of all Ministers of State. Initiatives based on this Strategy will contribute to ensuring Japan's national security and advancing digital reform with the Digital Agency as the control tower for digital reform, while also strengthening the response capabilities and coordination of relevant organizations, thereby enabling public institutions to fulfill their roles through the effective use of limited resources.

At the same time, in addition to establishing the National Cyber Director, the National Cybersecurity Office was established within the Cabinet Secretariat as the control tower for ensuring cybersecurity across the public and private sectors, including national security in cyberspace. The National Cybersecurity Office, serving as the secretariat of the Headquarters, plays a leading role in the comprehensive coordination across ministries and agencies, including those responsible for critical and essential infrastructure and those implementing remote access and neutralization measures. In particular, with regard to initiatives related to national security in cyberspace, the National Cybersecurity Office, headed by the National Cyber Director, who concurrently serves[56] as Deputy Secretary General of the National Security Secretariat, will act as the control tower, carrying out robust, comprehensive coordination in close cooperation with the National Security Secretariat. Additionally, when necessary, the National Security Council will hold discussions and make decisions.

Furthermore, each ministry and agency will promote measures based on this Strategy, while reviewing and adapting more effective approaches in light of developments in the situation surrounding cyberspace. At the same time, they will strive to develop and strengthen the necessary systems and frameworks to promote these measures.

Furthermore, public–private collaboration and international collaboration are indispensable in promoting measures based on this Strategy. In addition to the National Cybersecurity Office, relevant ministries and agencies will actively promote public–private collaboration and international collaboration to enhance the effectiveness of these measures. Furthermore, in order to gain the understanding and cooperation of citizens, businesses, and the international community regarding Japan's initiatives, ministries and agencies will work in close coordination to actively disseminate this Strategy, related initiatives, and their effects to stakeholders both in Japan and overseas.

In the future, in order to ensure the effective implementation of this Strategy, the Headquarters will formulate an annual plan for each fiscal year while ensuring consistency with other relevant strategies, verify the progress of the measures, compile the results into an annual report, and reflect the findings in the annual plan for the following fiscal year.

[56] Article 16, Paragraph (7) of the Cabinet Act (Act No. 5 of 1947)

Furthermore, with regard to verifying policy progress, in addition to evaluations of the government's cybersecurity initiatives conducted through audits of government agencies and related agencies as previously implemented, evaluations will also be conducted of initiatives based on the common cybersecurity standards for critical infrastructure, positioned as a function of the Headquarters under the amended Basic Act, as well as of the status of cybersecurity assurance within government agencies and related agencies. These efforts will contribute to the steady improvement of cybersecurity measures by government agencies, critical infrastructure operators, and other relevant entities.

Furthermore, the legal framework, including laws and regulations related to cybersecurity, will be continuously reviewed in light of the implementation status of the Cyber Response Capability Strengthening Act and Necessary Arrangement of Relevant Acts, the implementation and evaluation of this Strategy and measures based on it, and changes in the cybersecurity environment.

Although this Strategy sets out the goals and implementation policies for various measures to be implemented over a period of approximately five years from its formulation, it does not preclude the agile implementation of measures not listed in this Strategy. On that basis, taking into account the environment surrounding Japan and the international situation, changes in socio-economic structures driven by technological innovation, and trends in various related strategies, this Strategy will be examined and reviewed as necessary, and revisions will be considered as appropriate.