(Provisional Translation)

Outline of Japan's Next Cybersecurity Strategy

(Note)

Japan is now revising the current Cybersecurity Strategy 2018 and decides on its New Strategy by the end of this year. This document shows its outline discussed at the Cybersecurity Strategy Headquarters held on May 13, 2021.

Cybersecurity Strategy 2018
https://www.nisc.go.jp/eng/pdf/cs-strategy2018-en-booklet.pdf

Outline of Next Cybersecurity Strategy (Japanese)
https://www.nisc.go.jp/conference/cs/dai28/pdf/28shiryou01.pdf

As of July 8, 2021

Introduction

- The next Cybersecurity Strategy to be formulated based on the Basic Act on Cybersecurity (hereinafter referred to as the "Basic Act") will be the third one, and it has been six years since the Basic Act was enacted in 2015. During this period, cyberspace itself has both expanded in quantity and evolved in quality, becoming increasingly integrated with the real space. It is safe to say that Japan has entered an era of Cybersecurity for All, in which cybersecurity must be ensured for all the people, business sectors, local communities, etc.

- This strategy will set out the goals and implementation policies of the various measures that must be taken in the next three years during the early 2020s. These goals and policies will be provided from a medium- to long-term perspective and based on an understanding of the times as outlined below. At the same time, this strategy will communicate to all stakeholders, foreign governments, and attackers Japan's commitment to ensuring cybersecurity based on the lessons learned from the response to the unprecedented coronavirus pandemic, digital transformation, and the experience to be gained through the handling of the Tokyo 2020 Olympic and Paralympic Games (hereinafter referred to as the "Tokyo Games") to be held this year.

1 Social and Global Context Surrounding Japan in the 2020s

(i) Changes in the economic and social landscape—spread of digital economy and promotion of digital transformation

- The rise of the internet has led to the creation of a new space called "cyberspace," and the great advancement of the digital economy through the Heisei era (1989–2019).

- The impact of the digital economy has affected people's everyday life. In Japan, about 90%[1] of the people use the internet today for an average of more than two hours a day.[2] People's behavior has changed, including the growing use of IoT, AI, 5G, and cloud services, diffusion of remote working, and implementation of e-learning, and cyberspace has become a foundation of economic and social activities for everyone. There are growing expectations for the realization of Society 5.0,[3] in which cyberspace is integrated with real space at a high level.[4]

- The Digital Agency will be established to lead the effort to create a digital society, and promote digital transformation under the vision of creating "a society where people can choose services that suit their needs and realize diverse forms of happiness through the use of digital technology," with the aim of achieving "people-friendly digitalization, with no-one left behind."

---

[1] Data from the 2019 Communications Usage Trend Survey (published on May 29, 2020) conducted by the Ministry of Internal Affairs and Communications. Internet users account for 89.8% of respondents overall, and over 50% of respondents aged 80 and above.

[2] Data from the FY2019 Survey Report on Usage Time of Information and Communications Media and Information Behavior (published on September 30, 2020) conducted by the Institute for Information and Communications Policy of the Ministry of Internal Affairs and Communications.

[3] Society 5.0 is the 5th stage of human history, following the hunting society, agricultural society, industrial society, and information society. It is a society in which new value and new services are created continuously bringing wealth to the people of society. (Source: Growth Strategy 2017 (Cabinet Decision on June 9, 2017)

[4] Some argue that an era of "cyber-physical space" is already here.

(ii) Expectations for contribution to SDGs

- It is expected that the realization of Society 5.0 will usher in a better, more enriched society where many of the current issues are solved, and contribute to the fulfillment of the SDGs adopted by the UN.
- The use of digital technology, including smart grid and automated manufacturing, is vital in Japan's effort to achieve green growth as well.

(iii) Changes in the national security environment

- The uncertainty surrounding the existing order that Japan has enjoyed is increasing rapidly. Changes in the international community are accelerating and becoming more complex, including the emerging interstate competition in the spheres of politics, economy, military affairs, and technology.
- Cyberspace has become an area of international interstate competition that reflects geopolitical tensions, even during normal times. The circumstances surrounding cyberspace have taken on an appearance that is neither peacetime nor wartime. As greater segments of society become increasingly digitalized, these circumstances have the risk of rapidly developing into a graver situation.
- In addition, differences in fundamental values concerning cyberspace and conflicts over international rules, technological foundations, data, and other matters are emerging as well.

(iv) Impact and experience of COVID-19

- The new lifestyle that has become the "new normal" partially embodies the realization of Society 5.0. Initiatives such as remote working, online education, and telemedicine are accelerating through compelling response to the pandemic.
- This process is also expediting the use of new services that leverage personal data.

(v) Application of efforts toward the Tokyo Games

- Efforts made by the public and private sectors toward the Tokyo Games will be applied in raising Japan's overall level of cybersecurity capabilities to better prepare for future large-scale international events, such as the EXPO 2025 Osaka, Kansai, Japan.

2 Japan's concepts

2.1 Cyberspace to be ensured

- The global expansion and development of cyberspace has turned it into a place where a wide range of information and data, both in terms of quality and quantity, can be freely generated, shared, analyzed and distributed across national borders regardless of time and place.
- Equipped with these characteristics, cyberspace offers a place where people can enrich their lives and realize diverse values by creating intellectual assets such as technological innovations and new business models. As such, it serves as a foundation for the sustainable development of the economy and society in the future while underpinning liberalism, democracy, and cultural development.
- To serve the purpose of the Basic Act by making cyberspace "a free, fair and secure space," the government has formulated a "Cybersecurity Strategy" based on this Act twice so far. This strategy defines Japan's basic plan for its measures on cybersecurity.
- Given an understanding of the era as discussed above, there is no reason to assume that the purpose of this strategy and its stance to cyberspace should be changed in any way. Rather, it should be understood the need to ensure "a free, fair and secure space" is greater than ever now when securing cyberspace is at risk.

2.2 Principles

- With this understanding, Japan will firmly maintain and abide by the five principles upheld in the past strategies as the basic principles to be followed in formulating and implementing measures on cybersecurity.

(i) Assurance of the free flow of information

- For the sustainable development of cyberspace as a place for creation and innovation, it is imperative to build and maintain a world (a world where "Data Free Flow with Trust" is ensured) in which transmitted information reaches the intended recipient without being unfairly censored or illegally modified en route.
- As a basic condition for the free flow of information in cyberspace, morality and commonsense, including consideration for privacy, are requested not to offend rights and interests of others.

(ii) The rule of law

- As the integration of cyberspace and real space progresses, the rule of law should also be maintained in cyberspace, which has developed as a foundation underpinning liberalism, democracy, and so forth, in the same way as in real space.
- Similarly, existing international law including the UN Charter should be applied in cyberspace, and any act that threatens peace and activities that support such acts should not be condoned.

(iii) Openness

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

(iv) Autonomy

- It is inappropriate and impossible for a nation to take on the entire role of maintaining order in cyberspace to sustainably develop as a space where order and creativity coexist.
- To maintain order in cyberspace, various social systems should autonomously fulfill their roles and functions, thereby increasing society's resilience as a whole and deterring the activities of malicious actors.

(v) Collaboration among multi-stakeholders

- 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 of international affairs.
- To meet the expectations of the people, cybersecurity policies should safeguard their free economic and social activities, secure their rights and convenience, and protect them by deterring the activities of malicious actors through law enforcement and legal systems in a timely and appropriate manner. Japan will make it clearer than ever that the nation possesses political, economic, technological, legal, diplomatic, and all other viable and effective means as national options.

3 Issues in cyberspace

- Cyberspace itself has both expanded in quantity and evolved in quality through the spread of digital economy and promotion of digital transformation, and contact points with real space have expanded to cover broader areas. Moreover, cyberspace has become increasingly positioned as an important public space where all people, regardless of age, gender, or geographic location, participate to engage in social and economic activities autonomously. In addition, in circumstances where various services are offered in cyberspace, the interconnection and interrelationship between the stakeholders have evolved as a result of the popularization of the cloud services, the increased complexity of supply chains, and other factors.
- Japan is aiming to realize the digital transformation's vision of creating "a society where people can choose services that suit their needs and realize diverse forms of happiness" through the use

of IoT, AI, 5G, mobility innovation, AR/VR, and other cutting-edge technologies, and the establishment of the new lifestyle that has become the "new normal."

- On the other hand, the use of digital technology presents new challenges as well. If used inappropriately with malicious intent, it can deepen the rift and increase risks between nations, suppress human rights, and expand inequality.[5] Risks which were unforeseen previously can also be increased, and such changes are advancing in a discontinuous manner due to the coronavirus pandemic, generating concerns about such risks to emerge in unexpected ways. While cyberspace continues to transform into a public space amid this context, the people continue to harbor a sense of anxiety about cyberspace.[6]
- To ensure "a free, fair and secure cyberspace" in these circumstances, it is needed to clarify the issues that must be addressed and promote policies based on a proper understanding of the risks that arise from the changes that are currently unfolding, or changes that could occur in the near future. Naturally, it is extremely important to consider medium- to long-term perspectives at the same time as service providers change every few years in cyberspace, which means that stakeholders that play a major role in ensuring cybersecurity can also change.

3. 1 Increase in risks in cyberspace

3. 1. 1 Risks from the perspective of environmental changes

- Environmental changes may be accompanied by increased threats and vulnerabilities of the society as a whole.

(i) Threat Perspective

- While cyberspace may allow us to enjoy the benefits of new technological innovation, this also means that the people will be putting much more information about themselves than ever before on cyberspace. Information that has bearing on their lives, bodies, and property will become increasingly subject to cyberattacks.
- It is also conceivable that attackers will take advantage of the fruit of technological innovation, such as automatic attacks using AI and autonomous attacks that do not rely on human control, which leads to greater threats.

(ii) Vulnerabilities of the society as a whole

- From the perspective of the society as a whole, the advancement of digitalization has inevitably involved companies in various industries and business categories that were hitherto unrelated to cyberspace, and even individuals including the young and elderly, to participate in

[5] This is also presented as a new challenge in the "Declaration on the commemoration of the seventy-fifth anniversary of the United Nations," and addressing digital trust and security is considered a priority.

[6] According to a questionnaire survey conducted by the Metropolitan Police Department in September 2020, 75.3% of respondents say they feel anxious about cybercrime.

cyberspace. While it is expected that cyberspace will become a space where everyone can participate with a sense of trust, gaps in literacy about cybersecurity and shortage or uneven distribution of workforce may be targeted by attackers as potential vulnerabilities.

- Furthermore, shortage of human resources in business organizations and the technology field may lead to a situation in which Japan must rely excessively on foreign sources for products, services, and technology related to cybersecurity. The lack of literacy also poses the risk of creating new vulnerabilities through the misuse of devices and services.
- Meanwhile, as services become more sophisticated, gaps formed in the process of coordinating digital services may become vulnerabilities for attackers to target, unless appropriate security measures are implemented.
- In addition, as everything becomes connected to networks through increased use of cloud services, expansion and widespread adoption of products and services delivered through complex global supply chains, and greater use of IoT devices among industries, the impact of incidents on economic and social activities may affect a broader and more diverse range of stakeholders and situations, making it increasingly difficult to solve.
- Moreover, the growing use of cloud services, combined with the expansion of remote work, is revealing the limitations of the traditional concept of boundary protection.

3. 1. 2 Risks from the perspective of international affairs

- As cyberspace has become a realm of interstate competition, and due to anonymous, asymmetric, and cross-border nature of cyberattacks, there are increasing threats of organized and sophisticated cyberattacks, including those suspected of being state-sponsored, with the aim of service disruption of critical infrastructure, theft of personal information and intellectual property, and interference with democratic processes.
- As wider sections of the economy and society are rapidly becoming digitalized, an increase in these types of cyberattack poses the risk of creating a graver situation that undermines the people's safety and security as well as the foundation of a nation and democracy, resulting in evolving into an issue of national security. Cyberattackers are becoming increasingly adept at hiding and disguising their identities. In particular, cyber activities suspected of state involvement include cyberattacks presumed to be conducted by China to steal information from companies related to the military industry and possessing advanced technology, and by Russia to exert influence to achieve military or political aims. North Korea also conducts cyberattacks to achieve political aims or obtain foreign currency. In addition, it is observed that China, Russia and North Korea are continuing to build the cyber capabilities of their military and other institutions[7].

[7] For details, please see "4.3 Contributing to the Peace and Stability of the International Community and Japan's National Security"

- In addition, as conflicts arise over international rules and other matters concerning cyberspace, some states are asserting that national governments should strengthen management and control of cyberspace. If this becomes the mainstream for international rules, it may become an obstacle to ensuring “a free, fair and secure cyberspace” that underpin Japan’s national security and principles to be followed.
- As national security has been expanding its scope to economic and technological fields, the struggle for technological supremacy is emerging, and some states are stepping up collection, management, and control of data.
- Moreover, as the supply chains for systems comprising cyberspace become increasingly complex and globalized, the risk of malicious functions, etc. getting embedded in products somewhere along the supply chain is arising. Similarly, risks related to the reliability and stable supply of cyberspace itself (i.e., supply chain risks), including disrupted supply of devices and services due to the state of political and economic affairs, are emerging as well.
- In this way, more and more organizations and individuals are becoming exposed to threats, and the means of cyberattacks are becoming organized and sophisticated, which undermine the stability of cyberspace. This situation has emerged as a common and urgent issue for the international community that is extremely challenging to solve for each stakeholder and state alone, putting at risk Japan’s aim of ensuring “a free, fair and secure cyberspace” on a global level.

3. 1. 3 Recent trends of threats in cyberspace

- Such trends are evident from observing recent stream of threats in cyberspace.
- Many attacks suspected of involvement of crime organizations or states are taking place. Overseas, attacks targeting elections and other forms of interference with democratic processes and large-scale attacks exploiting vulnerabilities in supply chains, are prevalent.
- Moreover, the popularization of remote working has led to increased cases of network intrusions via individual devices or through exploitation of vulnerabilities in VPN devices, and cases in which cloud services become targets of attack. In fact, cyberattacks that take advantage of current environmental changes have been observed, including those that target vulnerabilities created in the pandemic and attacks via overseas branches in line with globalization.
- In addition, Advanced Persistent Threat are continuing to do damage, as evidenced by the fact that indiscriminate attacks rapidly increased in 2020. Existing threats are also becoming more complicated and sophisticated, as can be seen in “double extortion” ransomware attacks that request money in return for restoring data and stopping the disclosure of stolen data. As background to this, it is pointed out that an ecosystem has become established to enable the provision of malware and collection of ransom to be carried out in a systematic manner, so that those with malicious intent can easily launch an attack even if they do not have sophisticated skills.

- These types of cyberattack are causing major impacts on economic and social activities by halting production activities, causing service disruption, doing financial damage, and stealing personal and confidential information.

3. 2 Issues and direction—Cybersecurity for All

- In the future, all stakeholders, including those that previously had no connections with cyberspace, will participate in cyberspace in one way or another. Given this situation, it is necessary to pursue initiatives aimed at ensuring cybersecurity "which no one left behind," in response to digitalization.
- With this mindset, Japan will push forward with measures to ensure "a free, fair and secure cyberspace" in an increasingly uncertain environment, in keeping with the understanding of issues and direction stated below.
- This understanding and direction concern the aims set forth in the Basic Act—"enhancing socio-economic vitality and sustainable development," "realizing a digital society where people can live with a sense of safety and security," and "contributing to the peace and security of the international community and Japan's national security"—and in light of an understanding of the current situation as stated above, the idea must be kept in mind in implementing measures to achieve any of these aims.

(1) Advancing digital transformation and cybersecurity simultaneously

- Currently, discussions are underway to establish the Digital Agency to lead the effort to create a digital society. Along with other initiatives, this represents a perfect opportunity to greatly promote digitalization in the economy and society as a whole.
- On the other hand, unless awareness of cybersecurity is raised and trust is built in the technological foundation and data that compose cyberspace, participation and commitment will not be gained within the current trend of digitalization, resulting in only achieving superficial digitalization that is not accompanied by real transformation. Conversely, properly addressing risks that change along with digitalization may also lead to increased awareness and trust regarding cybersecurity.
- Looking at the activities of individual companies, the ability to respond to IT systems and digitalization is forming a source of added value for operations, products, and services, as the world becomes increasingly digitalized. As such, ensuring cybersecurity will be an activity directly linked to corporate value. Moreover, at a time when speedy and flexible development and response are becoming increasingly necessary, the concept of "Security by Design," which represents the idea of ensuring cybersecurity in the planning and design stages of operations and systems of products, services, etc., will become more important than ever. It is also believed that digital investments and security measures will become increasingly integrated.

- In this way, it is important to promote digitalization along with efforts to ensure cybersecurity ("DX with Cybersecurity"). All stakeholders must pursue their initiatives with this understanding. As a nation, Japan will work to create a foundation that will serve as a basis for those initiatives and powerfully support moves to promote digitalization in other ways as well.

(2) Ensuring the overall safety and security of cyberspace as it becomes increasingly public and interconnected

- In past cybersecurity strategies, Japan encouraged public and private sector initiatives based on the three approaches of "mission assurance" of service providers," "risk management," and "participation, coordination, and collaboration" toward the sustainable development of cyberspace.
- In an environment of increasing uncertainty due to growing threats in cyberspace, emergence of vulnerabilities, changes in Japan's national security environment, and other factors, cyberspace must have the same level of safety and security as real space in order to be recognized as a public space. To this end, Japan must deepen and enhance all three approaches without overlooking the asymmetrical situation with the attackers, and work to improve the environment and address the causes. This requires all stakeholders involved in cyberspace to expect greater roles, and while independent efforts ("self-help") and close coordination among multiple stakeholders ("mutual help") continue to be important, Japan will continuously examine the role of each stakeholder, including the role of "public help" that serves as their foundation, and what to defend, and then enhance multi-layered approaches. At the same time, Japan will clarify the missions (functions) of national CERT[8] (CSIRT), while improving and enhancing them through examination so that the missions will be thoroughly fulfilled.

(i) Deepening "mission assurance" (ensuring trustworthiness of the entire value chain with a focus on securing delivery of services to end users)

- Traditionally, the idea of "mission assurance" has been positioned as an approach for service providers to steadily perform operations that must be performed as a "mission," with a focus on the direct users of services, in particular those under a contractual relationship.
- In recent years, the popularization of cloud services and increased complexity of supply chains have led to the delivery of various services through cyberspace. With many players participating in supply chains and the reliance on cloud service providers increasing, it is becoming increasingly difficult for end users to see who is responsible for services and operations. It is also becoming difficult to foresee the impact and repercussions that will result in the event of an incident. Taking cloud services as an example, the impact may now extent not only to businesses that use them, but also to the end users who use the services of those

[8] In the current strategy formulated in 2018, it is defined as "a coordinator / coordinator to deal with cyberattacks all in Japan together". Generally, CSIRT is an abbreviation for Computer Security Incident Response Team, and CERT is an abbreviation for Computer Emergency Response Team.

businesses. In these circumstances, the impact will be all the greater for individuals who used to have little involvement with cyberspace but must now inevitably participate in it as a result of the progress of digitalization. Accordingly, entities that use cyberspace to perform operations or provide services are required to act with the reliability of the entire value chain in mind.

- "Mission assurance" should continue to be important and promoted. This should be further deepened so that all organizations, as an entity that provides and composes cyberspace, will recognize ensuring the trustworthiness of the entire value chain from the operations and services that they must perform to the end users, as their "mission." By doing so, Japan will aim to create an environment where the safety and trustworthiness of the various products and services composing cyberspace are ensured, so that users can continue to use them with a sense of trust.

(ii) Improving "risk management" efforts

- With the increased threat of organized and sophisticated cyberattacks, Japan will cooperate with foreign governments and the private sector on various levels as it works to supplement the "risk management" of individual stakeholders and effectively strengthen efforts further.
- Specifically, Japan will actively defend against cyberattacks while making efforts to constantly review anticipated risks and ensuring the possibility of tracking attacks after they occur, in light of the trend of threats.
- Cyberspace is used as a key channel for stealing the personal information, information concerning intellectual property, which is a source of international competitiveness, and information related to national security. Given this situation, Japan will strive to ensure the trustworthiness of the technological foundation that composes cyberspace while also dealing with such cyberattacks.

(3) Enhancing initiatives from the perspective of Japan's national security

- The environment surrounding Japan's national security is becoming increasingly harsh, and cyberspace has become an area of interstate competition. Amid these circumstances, the asymmetrical situation with attackers in cyberspace must not be overlooked.
- While also having each stakeholder clarify such stance, Japan will strengthen its defense capabilities by securing the nation's resilience through enhanced capabilities of the Self-Defense Forces and other government institutions. At the same time, Japan will enhance deterrence capabilities to detect, investigate, and analyze cyberattacks so that Japan can identify the attackers and hold them accountable. As for cyber threats, in close coordination with our ally and like-minded countries, Japan will utilize political, economic, technological, legal, diplomatic, and other viable and effective means and capabilities, and take resolute responses.

- In addition, Japan will counter efforts intended to prevent the healthy development of cyberspace in cooperation with our ally, like-minded countries, and private organizations, and play an active role to ensure “a free, fair and secure cyberspace” globally, in a way that contributes to Japan’s national security.

4 Policy approaches toward achieving the objectives

- The following are targets and guidelines of the policies to be implemented in the coming three years based on the understanding of issues discussed in the preceding sections, with the aim of achieving the objectives set forth in the Basic Act.

4. 1 Enhancing socio-economic vitality and sustainable development—Advancing DX with Cybersecurity

-Japan’s society and economy must achieve digital transformation accompanied by various innovative changes in order to achieve the vision of creating “a society where people can choose services that suit their needs and realize diverse forms of happiness through the use of digital technology.”

- As the opportunities and impacts brought by digital transformation affect all stakeholders without exception, they must be aware of DX with Cybersecurity, and related initiatives must be advanced in all respects.

- These initiatives include efforts to raise the awareness of executives and other members of the economy and society, as well as improving literacy. In addition, from the perspective of advancing the independent efforts of each stakeholder, we will also pursue initiatives to promote DX with Cybersecurity among local communities and small and medium-sized enterprises (SMEs), and build a foundation for securing the trustworthiness of value chains.

4. 1. 1 Raising executive awareness

- The impact of COVID-19 accelerated the shift toward digitalization. Going forward, it will become important for companies to have a foundation for creating digital services with higher added value in order to remain competitive.
- It is assumed that executives must understand both digitalization and cybersecurity measures as basic skills and knowledge for management and basic matters underpinning core operations and revenue. As such, they must take full ownership and seek to achieve them both simultaneously. Cyber risks will no longer serve as an excuse for not working on digitalization.
- We will work to promote practices such as ascertaining risks and disclosing corporate information by ensuring that efforts to strengthen cybersecurity in line with digitalization are visualized through the practice of digital management guidelines and use of tools so that investors and other stakeholders who value sustainability will be aware of them, and also by offering incentives for such efforts.

- Moreover, we will push forward with efforts to create an environment where people can gain "Plus Security" knowledge[9] so that executives who pursue cybersecurity measures along with digitalization through such initiatives as those stated above can identify the risks inherent in the digital services that are the source of their company's competitive strength.

4. 1. 2 Advancing DX with Cybersecurity among local communities and SMEs

- As businesses are forced to respond to the pandemic, business models, workstyles, and employment patterns are changing as well. Against this background, opportunities for digitalization will spread to local communities, SMEs, and various industries and business categories that were previously unrelated to cyberspace, without exception.
- On the other hand, SMEs will face a lack of resources (expertise and talent) in their effort to pursue cybersecurity measures along with digitalization due to a difficulty deploying staff specialized in security.
- We will roll out community activities across Japan based on the idea of mutual help, and promote efforts to create opportunities for communities faced with a lack of resources to address issues and generate added value, not only through consultation with experts but also by matching businesses and human resources and developing talent.
- In order to make inexpensive, effective, and accessible security services and simple insurance products widely available for SMEs, we will advance efforts including operation of a system to evaluate and register services that meet certain criteria, in cooperation with industry-led consortium established with the aim of enhancing the cybersecurity of entire supply chains, including SMEs.
- In addition, we assume that widespread use of cloud services among SMEs will also become an important option going forward. Use of such services will entail a certain amount of risk that information may inadvertently be leaked due to the placement of information assets off company premises, as well as problems with settings, etc. Accordingly, we will communicate matters that cloud service users must keep in mind, and consider urging cloud service providers to take necessary steps to prevent or reduce configuration errors when using cloud services.

4. 1. 3 Building a foundation for ensuring trustworthiness of value chains

- While it is expected that all stakeholders will create new value by freely establishing value chains toward Society 5.0, in which cyberspace is integrated with physical space at a high level, new issues that will arise in such value chains will need to be addressed.
- In light of frameworks, etc., for security measures that are formulated with the aim of addressing such issues appropriately and cover both cyberspace and physical space, we will advance initiatives to create a foundation for building trustworthiness in value chains in Japan.

[9] This refers to knowledge that personnel who may not necessarily have expertise or work experience related to IT or security should acquire as needed, when such knowledge becomes necessary in collaborating with internal and external security experts.

(1) Supply chains

- As supply chains have become more complex and digital services more connected, it is now possible to build more flexible and dynamic supply chains. On the other hand, from the perspective of cybersecurity, the expansion of possible origins of cyberattacks and increased impact on real space are raising concerns, and it is becoming increasingly important to manage risks with a view of entire value chains.
- With this understanding, we will promote efforts to develop and implement concrete security measures in the industry by formulating both industry-specific and cross-industry guidelines based on the above frameworks, etc.
- We will also assist efforts made by consortium joined by organizations from various industries with the aim of strengthening cybersecurity measures across supply chains. Under this framework, we will also expand our activities to cover local communities and SMEs through supply chains, by evaluating, registering, and recommending services that target SMEs and meet certain criteria, and by visualizing the status of efforts to strengthen cybersecurity.

(2) Data flow

- In advancing various social and economic activities in cyberspace, it is important to secure the authenticity of data and reliability of the foundation of data flow that are the source of its value, including the perspective of ensuring data governance toward the realization of a Data Free Flow with Trust (DFFT)[10].
- Based on the characteristics of data whose attributes keep changing as it flows between different stakeholders, we will work to clarify the definition of data management (establishment of frameworks, etc.) from the perspective of identifying risk points.
- It is also necessary to create an effective mechanism for preventing spoofing of sources, falsification of data, etc. (hereinafter referred to as the "trust service"). With respect to the reliability of trust service, we will work on establishing and clarifying the requirements that must be fulfilled, evaluating their reliability, providing relevant information, and establishing frameworks for international collaboration (confirmation of interoperability with other nations), etc.

(3) Security products and services

- For independent efforts to spread, security products and services provided in the market must be trustworthy. Amid concerns about supply chain risks, it is believed that demand will grow

[10]The then Prime Minister Abe's speech, "Toward a New Era of 'Hope-Driven Economy' (tentative translation)," at the World Economic Forum Annual Meeting (January 23, 2019)

for objective third-party verification of the reliability of company products, etc., and such verification will become important as an industry.

- From these perspectives, we will work to build a foundation for ensuring reliability, nurture products and services made in Japan, and support overseas expansion by establishing a foundation for verifying the effectiveness of security products and services, and by evaluating and registering security services that meet certain criteria. We will also discuss how to visualize the reliability of verification service providers.

(4) Practical application of advanced technology and innovation

- As digitalization continues to advance, there will be an increasing need for security measures that are based on clear evidence and can be easily explained to parties within and outside organizations, or that make use of automation, etc. for greater efficiency. We must respond to the demand from society by advancing the establishment of a government-industry-academia ecosystem that facilitates active industry-academia collaboration, and by encouraging open innovation activities.
- Security products used in Japan are largely dependent on overseas manufacturers, making it difficult to accumulate the necessary know-how and knowledge for product and service development. As part of our effort to break through this situation, we will build an intellectual foundation for collecting, accumulating, analyzing and providing cybersecurity information within the country, and making it available as node for the industry and academia.
- In addition, we will develop and demonstrate a foundation for use with IoT systems and services across entire supply chains, and promote practical application with an eye to various industrial fields.
- As part of our effort toward the practical application of these new technologies, we will promote technical reviews aimed at the use of new technologies in government agencies.

4. 1. 4 Establishing digital/security literacy inclusively

- The foundation of cyberspace is becoming a basic infrastructure for people's lives. As we pursue "people-friendly digitalization, with no one left behind"[11] in this context, it is essential that the people acquire skills and basic knowledge (literacy) in cybersecurity so that they can use their own judgment to protect themselves from threats and enjoy its benefits in an inclusive manner.
- On the other hand, literacy is not something that can be gained overnight. Amid increasing opportunities to use various digital services and the advancement of efforts to digitalize the government, popularize the Social Security and Tax Number System, and implement the GIGA School Program, it is more important to encourage people to actively try using them and gain

[11] "Basic Policy on Reform toward the Realization of a Digital Society" (approved by the Cabinet on December 25, 2020)

experience than anything. We should implement various initiatives to accompany efforts to advance information education.

- Japan will take this opportunity to raise the awareness of the people through joint activities by the public and private sectors, in collaboration with efforts to support the use of digital technology. As for the advancement of the GIGA School Program, we will deploy “ICT assistants” who will help schools establish an ICT environment, enhance the ability to provide guidance on the use of ICT in teacher-training programs, and advance education on information ethics.
- With regard to the spread of disinformation on the internet, we will pursue wide-ranging efforts to raise awareness and encourage voluntary efforts by the private sector, given that such information can have an inappropriate impact on individual decision making and societal consensus building.

4. 2 Realizing a digital society where people can live with a sense of safety and security

- Cyberspace is evolving to become a public space where all stakeholders are involved, and the interconnection and interrelationship of socio-economic activities have been deepening across cyber and physical boundaries, while cyberattacks are becoming more organized and sophisticated.
- In light of this situation, all stakeholders are expected to engage in risk management through the coordination of various stakeholders in accordance with the transformation of the nature of cyberspace, thereby deepening the “mission assurance” approach declared under the basic vision of cybersecurity.
- The national government, in cooperation with various stakeholders, will build a secure and safe cyber environment for all stakeholders with better predictability. The national government will also constantly review its defensive measures and the key assets subject to defense against cyberattacks, and commit to their safety by using all means available to implement comprehensive cyber defenses.
- Through these initiatives, we will achieve a multi-layered cyber defense, that is based on self-help, mutual help, and public help, and which reduces risks and increases resilience for the entire country.

4. 2. 1 Providing a cybersecurity environment to protect the people and society

- The national government will work together with relevant stakeholders and pursue various initiatives to create an environment where the stakeholders can choose appropriate risk management options suited to their needs. The national government will also eliminate factors and environments that tolerate cybercrimes, and promote reporting to the police regarding their cybercrime situations. These efforts can be achieved by increasing traceability and visibility of

cyberspace which is compose of complex IT systems and where various socio-economic activities are interconnected.

- With the deepening of the interconnection and interrelationship between stakeholders across the boundaries of cyberspace and physical space, there is a risk that the impact of incidents will extend over a wide area and cause more damage than expected. For this reason, the national government will encourage all service providers in cyberspace to ensure safety and security with a broad view of entire supply chains, focusing not only on the immediate users but also on the users who exist further downstream.
- As for protecting the critical socio-economic infrastructure, the basic requirement will be for relevant stakeholders to ensure confidentiality, availability, and integrity according to their respective roles. However, given the changing nature of cyberspace as discussed above, it will become more and more difficult to achieve this goal only by means of self-help and mutual help. As such, the national government will work together with various stakeholders, take the attackers' viewpoints into account as well, and use all means available to implement comprehensive cyber defenses, thereby working energetically to reduce risks and increase resilience for the entire country.
- The personal information of the people and information concerning intellectual property, which is a source of international competitiveness, are important assets that the national government must protect. As cyberattacks that steal these types of information compromise the safety and security of the people and injure fair economic transactions, the national government will take comprehensive measures to protect those assets against cyberattacks from a perspective of economic security.

(1) Building a safe and secure cyber environment for users

- The national government will work together with relevant stakeholders and pursue various initiatives to create an environment where the stakeholders can choose appropriate risk management options suited to their needs, thereby contributing to enhanced risk management based on self-help and mutual help. As an example, we will work to increase the traceability and visibility of cyberspace through an integrated approach that encompasses both public and private sectors, while ensuring the confidentiality and privacy of communication.

(i) Establishing supply chain management grounded in cybersecurity

- To undertake necessary supply chain measures that include risk management from a perspective of supply chains, the government will promote efforts to develop and implement concrete security measures in the industry. This will be achieved through the formulation of both industry-specific and cross-industry guidelines based on a framework for security measures that cover both cyberspace and physical space.

- The national government will support industry-led initiatives aimed at promoting information sharing, reporting, and appropriate announcements within the supply chain, so that any risks that occur can be controlled by each actor with a broad view of the entire supply chain, including SMEs, overseas offices, and business partners.
- The national government will build a mechanism for securing the reliability of supply chain components including devices, data, and services. In addition, we will advance the construction of a mechanism for detecting and protecting against attacks that impair the maintenance and reliability of traceability, with the aim of continually maintaining trust in these components on the supply chain.

(ii) Ensuring safety and security in implementing new technologies and services including IoT and 5G

- Amid the rapid proliferation of IoT, we will work to realize a safe and secure IoT environment by identifying devices that may be exploited to carry out cyberattacks and alerting consumers. In addition, we will engage in collaborative activities, formulate guidelines, share information, advance international standardization, and establish a system for addressing vulnerabilities, all with the aim of achieving secure IoT systems based on the concept of security by design. Furthermore, in terms of the use of IoT devices and systems, it will be necessary to combine cybersecurity measures with measures taken from a perspective of safety, so we will advance the use of a framework that meets the requirements for such a combination of safety and security.
- We will promote the establishment of a mechanism for safeguarding the cybersecurity of national and local 5G networks, as well as the development, supply, and deployment of 5G systems that ensure cybersecurity.
- We will establish a system for addressing vulnerabilities by formulating guidelines and codes of conduct for cybersecurity in new fields, including autonomous driving, drones, automated factories, smart cities, crypto assets, and the space industry.

(2) Strengthening cooperation with new providers in cyberspace

- Cyberspace is ceaselessly and advancingly changing and new providers of services in cyberspace are constantly appearing as ever-improving technologies and services continue to be implemented. Under such circumstances, the national government will always monitor the new technologies and services in cyberspace, analyze their mutual impact on the stakeholders in cyberspace and the severity of the impact, and create an environment where each stakeholder can take responsible steps to safeguard cybersecurity.
- In particular, as cloud services are becoming an indispensable infrastructure in cyberspace, their users are facing difficulties which they cannot manage by themselves. For example, the users encounter unintended incidents due to cloud services' improper settings and they sometimes

cannot notice such incidents. Also, cloud services have such characteristics that most of their users may face the same incidents at the same time. To help government agencies and critical infrastructure operators, as cloud service users, safely and securely entrust their information assets to cloud services, the national government will facilitate drawing up a set of rules and guidance, which the users take into consideration when they design and develop information systems based on cloud services, in cooperation with the users, cloud service providers and system integrators, etc. To this end, users can choose the cloud services suited to their own risk management principles and certainly understand the cloud services' security policies and the demarcation point of responsibility. Moreover, such an environment can be created that they can appropriately deal with problems when users, providers and system integrators fail to understand each other. In parallel, the national government will broadly expand its work to visualize cloud services' safety from the government agencies to private sectors, by using the Information system Security Management and Assessment Program (ISMAP) and other similar initiatives, as well as promote global collaboration as many cloud services are provided by foreign companies.

- As for services used by many public institutions, companies, and individuals, we will promote cybersecurity measures including further supply chain management, considering their role as a social platform.

(3) Addressing cyber crimes

- In light of the fact that cyberspace is evolving to become a public space where all stakeholders are involved, the national government shall continue to push forward with the disclosure of criminals, who exploit cyberspace, and malicious business operators, who provide criminal infrastructure hindering traceability, with the aim of ensuring safety and security on the same level as in physical space.
- The national government will also prevent cyberspace from becoming a criminal infrastructure through public and private sector collaboration, leveraging information about infrastructure and technologies that are at high risk of being used to commit a crime as revealed through criminal investigations, and engaging with relevant business operators.
- The national government will also strengthen efforts such as cooperation with relevant business operators and international collaboration in order to remove environments and causes that tolerate the current asymmetric situation with attackers.

(4) Deploying comprehensive cyber defense

- In order to set up defenses against serious cyberattacks that undermine the safety and security of key assets such as the critical socio-economic infrastructure and lifeline, the national government will address in corporation with the relevant organizations, threat hunting,

handling incidents and taking preventive policy measures in an integrated manner by using all means and capabilities available as a national government.

(i) The national government will advance efforts to enhance the functions of national CERTs (CSIRT), beef up response capabilities by marshalling and coordinating the resources of responsible government agencies, and collaborate with information sharing organizations including the Cybersecurity Council and the Cybersecurity Response and Coordination Center. This will ensure that collaboration and coordination with external parties, collection and analysis of information, investigations, issuing alerts, formulating countermeasures and responses, and taking preventive policy measures will be implemented seamlessly and effectively, thereby enabling an active and exhaustive response as a nation.

(ii) The national government will work together and discuss measures concerning "Active Cyber Defense" including vulnerability handling, technical verification mechanism, and proper and timely damage announcements, as well as establishing functions for investigating the cause of relevant industrial control system incidents.

(5) Ensuring trustworthiness of cyberspace

- Given that many of the cyberattacks currently recognized target the personal information and intellectual property information which is a source of international competitiveness, the national government will take comprehensive protective measures against cyberattacks from a perspective of economic security.

(i) Efforts to support stakeholders that possess the personal information of the people and information concerning intellectual property

- We will seek thorough implementation of countermeasures by providing timely and appropriate information about effective safety management measures that protect personal information from cyberattacks.
- The national government will strengthen efforts in corporation with relevant organizations to promote information sharing by private companies, universities, and other actors that possess or manage the personal information of the people and information concerning intellectual property.

(ii) Ensuring trustworthiness of IT systems and services from the perspective of economic security

- The national government will advance measures to ensure the trustworthiness of IT systems and services that are embedded in critical socio-economic infrastructure with a major impact on our people's lives and economic and social activities, examining various risk scenario including supply chain risks as well.

- The national government will strengthen the protection of international submarine cables with international and public-private cooperation by ensuring safety, trustworthiness and redundancy.
- The national government will advance efforts to assure trustworthiness of IT devices and services through international collaboration including standardization, and establishing technical verification mechanism. The national government will enhance trustworthiness of IT devices and services procured by government taking supply chain risk into account.

4. 2. 2 Ensuring cybersecurity in close cooperation with digital transformation led by the Digital Agency

- To realize "people-friendly digitalization, with no one left behind," it is necessary to thoroughly improve usability from the people's perspective while also ensuring cybersecurity. For this reason, the basic principle for cybersecurity will be proposed in the Digital Agency's basic development and management principles (development policy) for the information systems of the national government, local governments, semi-public sector, etc. and will be implemented.
- From the perspective of safe and secure data usage, the Digital Agency will govern the planning of ID systems which uniquely identify individuals and corporations (e.g., Social Security and Tax Numbers, corporate numbers) and systems which ensure the authenticity of information and its provider (e.g., electronic signatures, electronic commercial registration certificates), in joint collaboration with relevant ministries, reform them from the user's viewpoint, and promote their utilization.
- The national government implements the ISMAP system, which supports the realization of the cloud-by-default principle, will update the system on an ongoing basis in light of the implementation status, and encourages its use by the private sector as well.

4. 2. 3 Promotion of efforts by stakeholders which underpin the socio-economic infrastructure (1) (Government agencies, etc.)

- Each government agency is conducting information security measures in conformity with the unified government security standards, while the national government is working to enhance the overall governmental security level through efforts including security audits based on the standards, CSIRT training as well as GSOC's monitoring for malicious activities. Each government agency will strengthen security measures in every phase, including the development and building phases of information systems, as an essential aspect of digitalizing the entire society.
- In particular, critical systems commonly used by the ministries will be maintained and operated by the Digital Agency on its own or jointly with each ministry, ensuring stable and continuous operation including security.
- Facing new security risk which has been brought by the spread of remote work ascribed to COVID-19 and the introduction of cloud services, the national government will implement

measures to ensure safe and secure realization of “new lifestyles.” In particular, the conventional “perimeter security model” is no longer adequate in some cases, so the national government will consider the suitable ways to design, operate, monitor and audit information systems under such cases as well as how to arrange structures and human resources that will help to handle them.

- Given that the recent cyberattacks have become increasingly complex and sophisticated, security measures have to be taken considering the overall supply chain where some subcontractors, including overseas offices and SMEs, may not have adequate measures and so may be targeted by cyberattacks. Therefore, the national government will push forward with effective information security measures that address such new threats while assessing the effectiveness according to the size of the organization and other factors.
- Specifically, as security measures aligned with the cloud-by-default principle, the national government will promote the revision and implementation of the unified government security standards in accordance with the expanding use of cloud services and consider enhancing the GSOC functions to enable cloud services’ monitoring.
- Moreover, the national government will steadily implement the fourth GSOC (FY2021 to FY2024) and conduct technical reviews and revision of the unified government security standards toward the implementation of security architecture with the continuous diagnostics and response, not limited to the conventional “perimeter security model”, while initiatively promoting the implementation in the government agencies from where possible. Also, the national government will discuss the roles and functions of the GSOC in terms of measures to address information security.
- The national government will strengthen the response to supply chain risks and IoT devices and services (including IoT of industrial control systems) in administrative areas.
- The national government will implement security measures (e.g., authentication function, default settings of cloud services, vulnerability countermeasures) that should be adopted at the phases of the design and development of information systems.
- The national government will maintain and improve the cybersecurity response among government agencies, etc. through security audits and CSIRT training, etc.

4. 2. 4 Promotion of efforts by stakeholders which underpin the socio-economic infrastructure (2) (Critical infrastructure)

- Our nation’s economy and society depend on the continuous provision of various critical infrastructure services. Given the increasing interdependency between critical infrastructures and increasing complexity and globalization of supply chains, a safe and secure society cannot be realized without safeguarding the cybersecurity of critical infrastructure, which is subjected to threats that increase year after year, and enhancing its resilience.

- The Basic Act on Cybersecurity, which was promulgated and enacted in 2014, clearly provides the responsibilities of critical infrastructure operators. The Act also provides that the national government must promote voluntary efforts including formulation of standards, exercises, training, and sharing of information with regard to the cybersecurity of critical infrastructure operators, etc., and implement any other necessary measures.
- In light of the above, we will ensure the stakeholders involved in critical infrastructure understand their responsibilities, and we will advance efforts toward the realization of robust critical infrastructure through a joint approach by the public and private sectors.

(1) Advancing protection of critical infrastructure based on public-private collaboration

- For the safe and continuous provision of critical infrastructure services, which form the foundation of people's lives and socio-economic activities, the public and private sectors will share a common policy between the national government, which bears responsibility for critical infrastructure protection, and critical infrastructure operators, which independently carry out relevant protective measures. This will serve as the basic framework for critical infrastructure protection, and we continue to promote these initiatives.
- Threats surrounding critical infrastructure are becoming increasingly advanced and sophisticated year after year. On the other hand, due to the difference in how systems are used in each field of critical infrastructure, the gap in threats faced by each organization is widening. With this understanding, we will base our efforts on the current "The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)" which serves as a reference for critical infrastructure protection, while also actively updating the policy to further enhance critical infrastructure protection based on public-private collaboration. This will enable critical infrastructure fields as a whole to flexibly respond to trends in future threats and changes in the environment surrounding systems and assets.
- For the safe and continuous provision of critical infrastructure services, digital technology will play a huge role, and safeguarding cybersecurity concerns the very foundation of business management. With this understanding, we will work to ensure that critical infrastructure services will be advanced, protected by appropriate security measures, and maintain a suitable balance between business and security. To this end, we will further enhance the system of cross-sectoral information sharing to facilitate information collection by critical infrastructure operators, etc., so that each organization can make effective use of lessons learned from prior examples. We will also build a system that will enable management to fully exercise leadership since it is important for the entire organization to work as one for security measures to be effective.

(2) Support for local governments

- Local governments hold vast amounts of sensitive information, including personal information, and provide basic services closely related to people's lives. In light of this fact, the national

government will provide necessary support to ensure proper security at local governments while considering the separation of roles between national and local governments.

- To ensure security measures are steadily implemented based on the “Guidelines for information security policy for local governments” (hereinafter referred to as the “Guideline”), we will support initiatives aimed at securing and training human resources, enhancing systems, and securing necessary budgets.
- We will continue to update the Guideline and advance efforts to establish necessary systems to be able to flexibly respond to the demands of a new era, such as standardization of local government information systems, handling administrative procedures online, promotion of the cloud in line with the “cloud-by-default principle,” and introduction of remote work as part of workstyle reform and business continuity.
- To promote digital transformation (realization of digital government) among local governments, the national government will establish a security policy for local governments in the maintenance policy, in light of the “Basic Policy on Reform toward the Realization of a Digital Society” (approved by the Cabinet in December 2020).
- With regard to the Social Security and Tax Number System, which closely relate to people’s lives and personal information, we will enhance countermeasures considering the balance between convenience and security, and promote safe and secure use.

4. 2. 5 Promotion of efforts by stakeholders which underpin the socio-economic infrastructure (3) (Universities, education and research institutions, etc.)

- Universities, inter-university research institutes, etc. (hereinafter referred to as the “universities, etc.”) consist of diverse members/organizations and own a wide range of information assets and systems. Given this situation, the national government’s active support for them to build collaborative and cooperative frameworks and information sharing is vital, along with their autonomously taking measures.
- The national government will initiatively help universities, etc. to establish and prevalently comply with cybersecurity guidelines, conduct seminars, training, and exercises on risk management and incident response, appropriately respond to initial response in the event of an incident, and cooperate among universities, etc., such as information sharing.
- With regard to the universities, etc. that possess cutting-edge technological information, the national government will comprehensively help them to enhance common security measures implemented through the entire organization as well as technological measures for protecting the technical information from advanced cyberattacks and effective measures against supply chain risks.

4. 2. 6 Strengthening seamless information sharing systems among various stakeholders and making use of findings obtained through efforts toward the Tokyo Games, etc.

- In light of the increasing risks in cyberspace, the national government will enhance risk sensitivity and resilience, advance timely, geographically and cross-cuttingly seamless information sharing and collaboration for effective and responsive handling of cyberattacks, and maintain an ability to respond immediately to large-scale cyberattacks even in peacetime.
- To enable comprehensive response as a nation against new attacks, the national government will leverage the findings and know-how obtained through efforts for preparation and operation for response capabilities and efforts for risk management for the Tokyo Games, as part of efforts to establish a national CERT (CSIRT) framework. By doing so, the national government will advance efforts to raise the nation's overall level of cybersecurity capabilities in peacetime, not just during large-scale international events, such as the EXPO 2025 Osaka, Kansai, Japan. The national government will also share the findings and know-how obtained through operations during the Tokyo Games with the international community in an appropriate way.

(1) Advancing information sharing and collaboration according to each field and issue

- The national government will enhance and strengthen existing efforts for information sharing, including ISAC, and help to establish and facilitate new mechanisms for information sharing under close collaboration with stakeholders in order to establish a multi-layered cyber defense system through coordinated collaboration between stakeholders in cyberspace.

(2) Establishing an information sharing and collaboration system that contributes to comprehensive cyber defense

- To enable comprehensive response as a nation against cyberattacks, the national government will strengthen collaboration between information sharing systems, including the Cybersecurity Council and the Cybersecurity Response and Coordination Center, as part of efforts to establish a national CERT (CSIRT) framework, and discuss the details of how to collaborate and coordinate with external parties.
- The national government will actively make use of the findings and know-how obtained through efforts for preparation and operation for response capabilities and efforts for risk management for the Tokyo Games so as to support the business operators assisting the operation of the Tokyo Games as well as nationwide operators' efforts for cybersecurity measures. By doing so, the national government will raise the nation's overall level of cybersecurity capabilities at all times, from during large-scale international events such as the EXPO 2025 to peacetime.

4. 2. 7 Strengthening readiness to respond to large-scale cyberattacks, etc.

- Given that cyberspace and real space are becoming increasingly intertwined and the impact of incidents may spread over a wide area, the national government will strengthen seamless and nation-united response capabilities even in peacetime, keeping in mind the possibility of a minor incident may escalate into a major cyberattack.
- The national government will strengthen response capabilities against cyberattacks in cooperation with communities in various fields and regions, while also enhancing information collection, analysis, and sharing functions through public-private collaboration.
- The national government and each organization will strengthen response to large-scale cyberattacks by training and utilizing security staff through public-private collaboration.

4. 3 Contributing to the Peace and Stability of the International Community and Japan's National Security

- Amidst the growing severity of the security environment surrounding Japan, the uncertainty surrounding the existing order that it has hitherto enjoyed is increasing rapidly. Changes in the international community are accelerating and becoming more complex, including the emerging interstate competition in the spheres of politics, economy, military affairs, and technology.
- Cyberspace has become a realm of competition that reflects geopolitical tensions, even during normal times.
- The situation in cyberspace can no longer be deemed purely peacetime nor wartime, as alleged cases of cyberattacks targeting the critical infrastructure of a state by a competent military unit of another country. As greater segments of society become increasingly digitalized, cyberattacks have the risk of rapidly developing into a graver situation.
- Influence operations, which are carried out using cyberspace that are difficult to attribute and assess incurred damages, can, at times, be conducted in combination with military operations and used in an attempt to change the status quo without engaging in armed attacks.
- In particular, cyber activities suspected of state involvement include cyberattacks presumed to be conducted by China to steal information from the military industry and possessing advanced technology[12], and by Russia to exert influence to achieve military or political aims[13]. North Korea also conducts cyberattacks to achieve political aims or obtain foreign currency[14]. In

[12] Review and Prospects of Public Order, Security Bureau, National Police Agency (December 2020), US National Cyber Strategy (September 2018), Cyber Strategy, US Department of Defense (September 2018)
In the "Overview of Threats in Cyberspace 2021" issued by the Public Security Intelligence Agency, it is indicated that the involvement of the Chinese military and intelligence agency has been pointed out.

[13] Review and Prospects of Public Order, Security Bureau, National Police Agency (December 2020), Cyber Strategy, US Department of Defense (September 2018)
In the "Overview of Threats in Cyberspace 2021" issued by the Public Security Intelligence Agency, it is indicated that the involvement of the Russian military and intelligence agency has been pointed out.

[14] Review and Prospects of Public Order, Security Bureau, National Police Agency (December 2020), Interim Report of the Panel of Experts Assisting the UN Security Council Sanctions Committee on North Korea (September 2019)
In the "Overview of Threats in Cyberspace 2021" issued by the Public Security Intelligence Agency, it is indicated that the involvement of the North Korean military has been pointed out in cyberattacks launched to gain money through malicious means, collect intelligence, and engage in destructive activities.

addition, it is observed that China, Russia and North Korea are continuing to build the cyber capabilities of their military and other institutions[15].

- Meanwhile, the United States, Japan's ally, and like-minded countries that share fundamental values have been accelerating efforts to build the capabilities of their cyber command and strengthen the ability to respond to cyberattacks[16].
- Under this background, countries share the importance of strengthening cooperation and collaboration with their allies and like-minded countries, and they are collaborating to address cyber incidents suspected of state involvement and conflicts over international rules in cyberspace in particular. In the Japan-US Security Consultative Committee (hereinafter referred to as the "Japan-US '2+2'") and Japan-US foreign ministers' meeting held in March 2021, the importance of further strengthening this field was confirmed.
- In addition, as national security has been expanding its scope to economic and technological fields in recent years to encompass economic and technological fields, we are likewise collaborating with our ally and like-minded countries to address conflicts over technological foundation and data as well.
- In this context, the importance of ensuring "a free, fair and secure cyberspace" and contributing to the peace and stability of the international community and Japan's national security has increased further. To ensure safety and stability of cyberspace, we will place a higher priority on cyber issues in diplomatic and national security agenda. At the same time, we will promote the rule of law, strengthen capabilities for defense, deterrence, and situational awareness against cyberattacks, and further enhance international cooperation and collaboration.

4. 3. 1 Ensuring "a free, fair and secure cyberspace"

- To ensure "a free, fair and secure cyberspace" on a global scale, we will communicate Japan's basic principles in the international arena and play active roles to advance the rule of law in cyberspace.

(1) Promoting the rule of law in cyberspace (formulating rules that contribute to Japan's national security)

- To ensure "a free, fair and secure cyberspace" on a global scale, we will continue to deliver the concept of "a free, fair and secure cyberspace" in the international arena and play active roles to promote the rule of law in cyberspace. In particular, cyberattacks targeting medical institutions are observed in many countries under the COVID-19 pandemic, so it has become even more important to advance the rule of law in cyberspace to deter such attacks and protect critical infrastructure.

[15] Defense of Japan 2020
[16] Defense of Japan 2020

- In the UN and elsewhere, we will collaborate with our ally and like-minded countries by actively engaging in the practice of norms in cyberspace, based on our stance that the existing international law applies in cyberspace as well.
- Through such activities, we will work to participate in discussion on the application of international law and promote the practice of norms both in Japan and abroad, thereby contributing to Japan's national security and efforts to increase the deterrence capability for the Japan-US Alliance as a whole.
- As for measures against cybercrimes, we will use existing international frameworks such as the Convention on Cybercrime and advance the universalization and enhancement of it. At the same time, we will promote the rule of law in cyberspace and further international collaboration through full involvement in discussion on the formulation of a new convention at the UN.

(2) Formulating rules in cyberspace

- In the G20 Osaka Leaders' Declaration, the need to promote Data Free Flow with Trust (DFFT) in a digital economy was confirmed, and the importance of trustworthiness in 5G security was mentioned in the Prague Proposals[17]. These examples show that moves toward international efforts based on collaboration among allies and like-minded countries are advancing. As for efforts to create order in the form of "a free, fair and secure cyberspace" that Japan is pursuing, frameworks based on a multi-stakeholder approach to internet governance such as the Internet Governance Forum are developing as well[18].
- Meanwhile, in light of the fact that proposals that may be incompatible with the existing order are being put forward, we will continue to deliver Japan's basic principles to the international community, and actively contribute to the formulation of new international rules in line with them. In addition, we will make every effort to ensure the formulation and implementation of such international rules contribute to the peace and stability of the international community and Japan's national security. We will work with our ally and like-minded countries, and private organizations to combat efforts aimed at changing international rules in a way that impedes the healthy development of cyberspace.

4. 3. 2 Strengthening capabilities for defense, deterrence, and situational awareness

- As the security environment surrounding Japan has become increasingly severe, it is vital to strengthen the capabilities to defend the nation from cyberattacks (defense capabilities), deter cyberattacks (deterrence capabilities), and be aware of the situation in cyberspace (situational awareness capabilities), while fundamentally enhancing the government's overall ability to respond seamlessly.

[17] The Prague Proposals refer to the Chairman Statement announced at the Prague 5G Security Conference in May 2019.
[18] The G7 Ise-Shima Leaders' Declaration (May 27, 2016) states, "We commit to promote a multi-stakeholder approach to Internet governance which includes full and active participation by governments, the private sector, civil society, the technical community, and international organizations, among others."

- The National Security Secretariat will be in charge of overall coordination for these initiatives related to national security. Under its coordination, all relevant public and private stakeholders led by NISC with regard to defense, the ministries and agencies responsible for response measures with regard to deterrence, and information gathering and investigative organizations with regard to situational awareness will closely cooperate even during normal times and proceed with the initiatives. When necessary, deliberation and decision will be made at the National Security Council.

-As a part of the government's overall effort concerning national security, the Ministry of Defense and the Self-Defense Forces (SDF) will undertake various initiatives based on the National Defense Program Guidelines for FY 2019 and beyond, and fundamentally strengthen cyber defense.

(1) Increasing defense capabilities

- From the perspective of mission assurance, government agencies and critical infrastructure operators, etc. must continue to advance efforts to ensure cybersecurity. The government will steadily conduct joint exercises by the SDF and US military to defend the critical infrastructure and services their activities depend on. The Ministry of Defense and SDF will strive to fundamentally strengthen cyber defense capability, for example, by enhancing the posture of cyber-related units.
- As information crucial to Japan's national security is being targeted, further measures including risk reduction is needed to protect technologies relevant to our national security, such as technology related to space, nuclear power, and other advanced technology. As for the defense industry in particular, we will advance efforts to maintain security by formulating new information security standards and further strengthening public-private collaboration. Moreover, the government will make further efforts to collaborate and share information and awareness of threat perception with relevant business operators that underpin Japan's national security, including critical infrastructure operators, industry players in advanced and defense technologies, and research institutions.
- We will continue to work together with the international community and implement necessary measures against the activities of terrorist groups exploiting cyberspace.

(2) Enhancing deterrence capabilities

- Cyberattacks could amount to the use of force or an armed attack[19] under international law. Based on this recognition, in order to deter malicious cyber activities and protect the people's safety and rights, Japan, in close coordination with our ally and like-minded countries even during normal times, will take resolute responses against cyber threats that undermine Japan's

[19] G7 Ise-Shima Summit, G7 Principles and Actions on Cyber (May 2016)

national security, including those possibly sponsored by states, utilizing political, economic, technological, legal, diplomatic, and all other viable and effective means and capabilities.

- In this regard, it was confirmed in the Japan-US "2+2" in 2019 that a cyberattack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the U.S.-Japan Security Treaty. In addition to employing capability to disrupt the opponent's use of cyberspace for the attack, during attack against Japan, we will take due steps including the use of diplomatic means and criminal prosecution[20]. For example, investigations of a case in which the police sent an investigation report to prosecutors in April 2021[21] led to the conclusion that the Chinese People's Liberation Army (PLA) was highly likely to be involved in the cyberattacks by a group with close links to the PLA against entities including Japanese companies.
- Since cyberattacks have the risk of rapidly developing into graver situation, we will quickly respond to incidents by seamlessly transitioning to the escalation of situation from peacetime to large-scale cyberattacks and then to armed attacks. In addition, we will continue to maintain and strengthen the deterrence of Japan-US Alliance, in light of the outcome of the Japan-US "2+2" in March 2021.
- The highly anonymous and covert nature of cyberspace has the risk of inadvertently heightening tensions among nations and aggravating the situation. Accordingly, it is important to establish an international communication channel from normal times as confidence building measures, in order to prevent accidental and unnecessary conflicts.

(3) Strengthening cyber situational awareness capabilities

- Situational awareness capabilities are the foundation of defense and deterrence capabilities.
- To identify attackers and hold them accountable, we will continue to improve the ability to detect, investigate, and analyze cyberattacks, and advance efforts to further clarify the actual situation of cyberattacks, leveraging the nationwide networks and technical units of relevant agencies.
- To address state-sponsored cyberattacks, we will advance information sharing among relevant ministries as well as with our ally and like-minded countries.

4. 3. 3 International cooperation and collaboration

- In cyberspace, the impact of incidents can easily transcend national boundaries, and cyber incidents that occurred in other countries can easily affect Japan. Accordingly, it is important to engage in multi-layered cooperation and collaboration on various levels, including foreign governments and the private sector.

---

[20] To date, we have issued a Press Secretary's comment in 2017 criticizing North Korea's involvement in WannaCry incidents, and in 2018 criticizing cyberattacks launched by a group called "APT10," which is based in China, working in collaboration with our allies and like-minded countries.

[21] A case in which the Metropolitan Police Department sent papers to the Tokyo District Public Prosecutors Office in April 2021, naming a Chinese Communist Party member as a suspect. In this case, it was concluded through investigations that the People's Liberation Army unit 61419, which is based in Qingdao, Shandong Province, was likely to be behind a cyberattack group called "Tick," which was suspected of launching a series of cyberattacks against approximately 200 Japanese companies.

(1) Sharing expertise and policy

- As conflicts over international rules and technological foundation come to the fore, we will strengthen collaboration with our ally and like-minded countries. This will include high-level cross-ministerial bilateral and multilateral talks including cyber dialogues with the US and like-minded countries, as well as multi-layered frameworks that enable the Cabinet Secretariat and ministries to engage in practical international collaboration with their counterparts from normal times.
- We will actively advance cooperation with the US, Australia, India, and other countries in the field of cybersecurity toward the realization of "Free and Open Indo-Pacific (FOIP)."
- We will also expand international collaboration concerning information sharing in the private sector, acquire human resources in the public and private sectors who can assert Japan's stance in the international arena, and develop human resources by dispatching them to other countries and sending them to participate in international conferences.
- In addition, we will enhance the communication of information about Japan's cybersecurity policies to international audiences, and we will make international contributions by sharing our experience at the Tokyo Games with other countries.

(2) Strengthening international collaboration for incident response

- To respond rapidly to cyber incidents and prevent the spread of damage, we will continue to enhance the sharing of information related to cyberattacks (e.g., information about vulnerabilities and IoC [22]) with international partners from normal times, and consider disseminating information jointly with other countries.
- We will enhance our international presence in the cyber community. To this end, we will not only promote collaboration among CERTs and participate in international cyber exercises, but we will also lead such exercises and build trust for collaborative response, as well as serving as an information hub.

(3) Cooperating for capacity building

- Other countries are providing various capacity building supports for developing countries. Under Japan's basic principles, we will provide the required supports strategically and efficiently as a nationwide effort, and also in a multi-layered manner in collaboration with diverse stakeholders including like-minded countries, international institutions such as World Bank, industry and academia.

[22] IoC (Indicator of Compromise) is information that indicates traces of cyberattacks.

- By ensuring cybersecurity in this manner, we will promote the achievement of the SDGs and help maintain cyber hygiene. Moreover, we will also support the capacity building not only through human resource development and cyber exercise, but also in understanding and practicing international legal principles, policy formation, and fields that form the next-generation cyber environment such as 5G and IoT.
- Additionally, we will boost overseas business expansion in cybersecurity field, in line with "Infrastructure System Overseas Expansion Strategy 2025." [23]
- In addition to these efforts, we will radically enhance collaboration in the Indo-Pacific region in particular, including ASEAN. It will include diplomacy and national security in the cyber field, based on Japan's achievements and experience of capacity building, in consideration of the region's geopolitical significance.
- We will update "The Cooperation for Cybersecurity Capacity Building in Developing Countries (The Basic Policy)[24]," which is the basic policy for capacity building, along with formulating the new cybersecurity strategy, with a view to enhancing efforts that include government-industry-academia collaboration, diplomacy, and national security.

4. 4 Cross-Cutting Approaches to Cybersecurity

- To achieve the three policy objectives set forth in the Basic Act, it is important to build a foundation by engaging in R&D, human resources development, and awareness-raising activities from a cross-cutting, medium- to long-term perspective.

4. 4. 1 Advancement of R&D

- We will work to strengthen international competitiveness and build a government-industry-academia ecosystem from a medium- to long-term perspective. At the same time, we will use these as a foundation to advance practical R&D while taking medium- to long-term technological trends into consideration.

(1) Strengthening international competitiveness in R&D and building a government-industry-academia ecosystem

- The field of cybersecurity research is new and growing, with the number of papers submitted growing rapidly around the world. This is a field where active collaboration is seen, such as international co-authorship and papers written for government-industry-academia projects. Combined with the expanding use of digital technology, this has become an important field of research.

[23] Finalized by the Infrastructure Strategy Economic Cooperation Meeting (December 2020)
[24] Cybersecurity Strategic Headquarters Report (October 2016)

- While the number of researchers has been increasing in Japan as well, social demands have grown even further thanks to the digitalization of the economy and society. To achieve the digitalization of Japan and enhance, develop, and fully supply our own cybersecurity measures and technology, we will promote research and government-industry-academia collaboration from a medium- to long-term perspective, strengthen international competitiveness in R&D, and build a government-industry-academia ecosystem.
- We will promote the research of relevant ministries and use of measures to promote government-industry-academia collaboration, while also striving to create an environment where researchers can engage in research with peace of mind by providing fully equipped research environments. In addition to advancing the widespread adoption and practical application of the results of R&D, we will also promote information exchange by relevant ministries toward the use of new Japan-made technology by government agencies as part of this effort.

(2) Advancing practical R&D

- Based on an understanding of current issues surrounding Japan (e.g., growing supply chain risks, providing cybersecurity with domestic resources), as well as a perspective of national security, we will advance practical R&D related to cybersecurity in the following direction.

  (i) Establish an all-Japan technical verification system for addressing supply chain risks

  (ii) Advance support measures for cultivating/developing domestic industries

  (iii) Enhance foundations for monitoring, analyzing, and sharing attacks

  (vi) Advance research of cryptography, etc.

- Advance the efforts of relevant ministries during the strategic period, follow up on the status of efforts including (1), and conduct inspections and any necessary re-arrangement by mapping efforts and so on.

(3) Taking medium- to long-term technological trends into consideration

- It is important to advance R&D based on a medium- to long-term perspective of technological trends, according to the progress of IT technology, including the development of "Beyond 5G"[25] and another advanced network technology. In particular, it will be necessary to take the progress of AI, quantum, and other advanced technology into consideration.

(i) Measures with a view to the advancement of AI technology

- Cybersecurity measures using AI (AI for Security) and responding to cyberattacks that use AI

[25] This refers to the further advancement of the characteristic features of 5G and addition of features that contribute to the creation of new, sustainable value.

- Security for protecting AI itself (Security for AI)

(ii) Measures with a view to the advancement of quantum technology

- Study of post-quantum cryptography
- R&D of quantum communications/cryptography that ensure safety in principle

4. 4. 2 Recruitment, development, and active use of human resources

- Given an understanding of the current situation regarding the lack of human resources and the spread of efforts toward digitalization, we need to further continue and deepen efforts by the public and private sectors both in terms of quality and quantity.
- Moreover, it is important to create an environment where cybersecurity personnel, regardless of gender, can play active and wide-ranging roles with diverse perspectives and excellent ideas, and to create a virtuous cycle that attracts talented human resources who will lead the next generation.
- Accordingly, we will create an environment that enables talented human resources to develop their careers spanning private sectors, municipalities, and government agencies, while responding to changes in the environment and focusing on efforts aligned with the following policy objectives.

(1) Advancing DX with Cybersecurity

- It is important to create a virtuous cycle driven by the demand and supply of human resources resulting from the advancement of digitalization in companies and organizations.
- For this to happen, business managers and DX champions must understand both digitalization and cybersecurity measures as basic matters underpinning core operations and revenue. As such, they must take full ownership and seek to achieve them both simultaneously. With this understanding, we will work to raise awareness while advancing the following initiatives.

(i) Providing "Plus Security" knowledge

- In advancing “DX with Cybersecurity” as a society-wide effort, it is extremely important to provide "Plus Security" knowledge to various human resources who may not necessarily have expertise or work experience related to IT or security, including management and executives, and ensure smooth collaboration with security experts both inside and outside the organization. At the same time, it is also important to secure human resources who can plan measures based on management’s policies and coach workers and engineers, and we will enhance “strategy management level personnel” through these efforts.

- To ensure human resources development programs such as training and seminars are implemented widely across society as part of such efforts, the national government and related agencies and organizations will conduct awareness-raising activities to stimulate demand. In addition, the national government will provide pioneering and fundamental programs, while also working to form and develop a market by matching supply and demand with respect to human resources development programs through a system in which a certain level of quality can be ensured and expected from the perspective of the user. These efforts will be accompanied by a focus on a foundation and environment for human resources development provided by the private sector, as well as “mutual help” initiatives through local community building.

(ii) Creating an environment where IT and security personnel can play an active role

- Digital transformation has seen an accompanying rise in the digitalization of work, network connection of products, development of digital services, and coordination between digital services. As a result, new development, monitoring, and response practices will become necessary, and the concept of security by design will become even more important in the future. Therefore, we will consider these trends and the even distribution of human resources as we promote practices related to building functions and securing and developing IT and security personnel inside companies and organizations.
- In terms of job opportunities for these human resources, we will see increasing use of alternative forms of employment such as secondary and concurrent employment, as well as a greater number of positions for digital transformation work at government agencies. To advance “DX with Cybersecurity” as a society-wide effort, we need to tackle it as a two-pronged approach. First, we need to ensure companies and organizations to conduct practices for building appropriate development, monitoring, and response functions tailored to the digitalization of work, products, and services. Then, we also need to create an environment that promotes the mobility and matching opportunities of IT and security personnel using the diversification of workstyles and employment patterns and the advancement of digital transformation as opportunities. Accordingly, we will actively share examples of practices suited to the new age as leading practices, and we will facilitate implementation by providing networks and know-how that will serve as a reference in practice.

(2) Addressing increasingly sophisticated and complex threats

- We are seeing greater numbers of sophisticated and complex cyberattacks, including those targeting industrial control systems, and as supply chains become increasingly complex and globalized, risks are growing as well. Against this background, developing human resources equipped with practical skills for handling such risks and attacks has become more important than ever.

- To address these developments in the threat landscape, we will enhance programs designed to develop human resources equipped with such practical skills, develop and improve relevant content, build a common foundation for the whole society to develop human resources specializing in cybersecurity, and make it available to stakeholders in industry and academia.
- To facilitate the career development of these human resources, it is also important to encourage people who completed these programs to form communities and interact with each other, pursue initiatives aimed at promoting the use of qualification systems, and advance efforts to secure experts at public institutions, including the police and Self-Defense Forces.

(3) Pursuing government agency initiatives

- From the perspective of facilitating the career development of IT and security personnel, it is important to create an environment that enables talented human resources to develop their careers spanning private sectors, municipalities, and government agencies. Based on this policy[26], we will present new measures to enhance the system for enlisting the help of advanced outside experts, quickly introduce a system that makes it easier to secure skilled human resources, and improve and enhance training, and then we will steadily advance these initiatives.
- Based on the human resources recruitment and development plan of each ministry, we will steadily work to establish an adequate system by increasing the quota, conduct training and exercises, and ensure appropriate treatment under the leadership function of the Deputy Director-General for Cybersecurity and Information Technology Management. In addition, we will review and update the plan each fiscal year and further enhance initiatives.
- In particular, to address advanced cybercrimes and national security, we will not only enlist the help of advanced outside experts but also develop and recruit our own advanced experts within government agencies.

4. 4. 3 Collaboration based on full participation and awareness raising

- As cyberspace and real space become increasingly intertwined, and cyberattacks increasingly sophisticated and complex, it will be vital for all the people to have an awareness and understanding of cybersecurity and to be able to address various risks, as with crime prevention and traffic safety measures in real space. It will be important to have the people acquire skills and basic knowledge (literacy) and, at the same time, raise awareness and provide information to reinforce behavior that allows them to protect themselves from threats using their own judgment.
- Getting various stakeholders to work together and collaborate in their own respective roles is more important than anything.

[26] "Basic Policy on Reform toward the Realization of a Digital Society" (approved by the Cabinet on December 25, 2020)

- With this understanding, we will formulate a detailed action plan so that stakeholders in industry and academia and the public and private sectors can engage in smooth and effective awareness-raising activities, and we will advance initiatives with a focus on local communities, SMEs, and young people. As the advancement of digital transformation leads to a wider range of people participating in cyberspace, we will push forward with the action plan and make ongoing improvements while considering updates in light of the situation.
- In addition, we will take necessary steps with respect to the nature (content) of information provision and awareness-raising activities, particularly as more and more people engage in remote work and use cloud services.

5. Promotion and Implementation of Cybersecurity

- A concerted effort by the whole government is needed to promote and implement cybersecurity in order to ensure a free, fair and secure cyberspace through our cybersecurity policies that we have discussed. Further efforts will be made to strengthen the capabilities and collaboration of relevant agencies so that initiatives based on this strategy can contribute to the digital transformation led by the Digital Agency, and that public agencies can make effective use of their limited resources to fulfill their roles. In these efforts, NISC will assume a key and leading role in coordinating the activities of ministries and promoting the collaboration of industry and academia and the public and private sectors, as the secretariat of the Cybersecurity Strategic Headquarters.
- Crisis management needs to be further enhanced as well. The Cybersecurity Strategic Headquarters will share information and collaborate with the Major Terrorism Response Headquarters and other crisis management organizations as needed. Problems that concern national security will be addressed by relevant ministries working together under the coordination provided by the National Security Secretariat, and through close collaboration with the National Security Council.
- NISC and relevant ministries must work together to actively communicate this strategy to stakeholders both in Japan and abroad so that it will lead to specific measures expected by the stakeholders in response to changing cybersecurity risks, and so that it will facilitate an understanding of the importance of international cooperation, the deterrent effects against attackers, and Japan’s stance toward other governments.
- Based on the direction indicated in this strategy, the Cybersecurity Strategic Headquarters will establish a policy for estimating expenses and work to secure and execute the necessary budget as the government so that the ministries can steadily and effectively implement their measures. Moreover, we will discuss the system needed to enhance the ability to quickly detect, analyze, assess, and address cyberattacks in an integrated cycle, building on the information collection and analysis function.
- Going forward, the Cybersecurity Strategic Headquarters will ensure this strategy is properly implemented by creating an annual plan for each fiscal year, verifying the progress of each

measure, summarizing the findings in an annual report, and reflecting them in the annual plan for the next fiscal year during the period of the three-year plan. Annual plans and reports should be discussed in an integrated manner, and the results and evaluation of the previous year's activities and the activities for the next year based on this strategy should be organized along matters outlined in this strategy so that the whole sequence of the reports and plans will be clear.