Cybersecurity Strategy

Cybersecurity for All

Cybersecurity which leaves no-one behind

The Government of Japan

September 2021

Contents

Cybersecurity for All

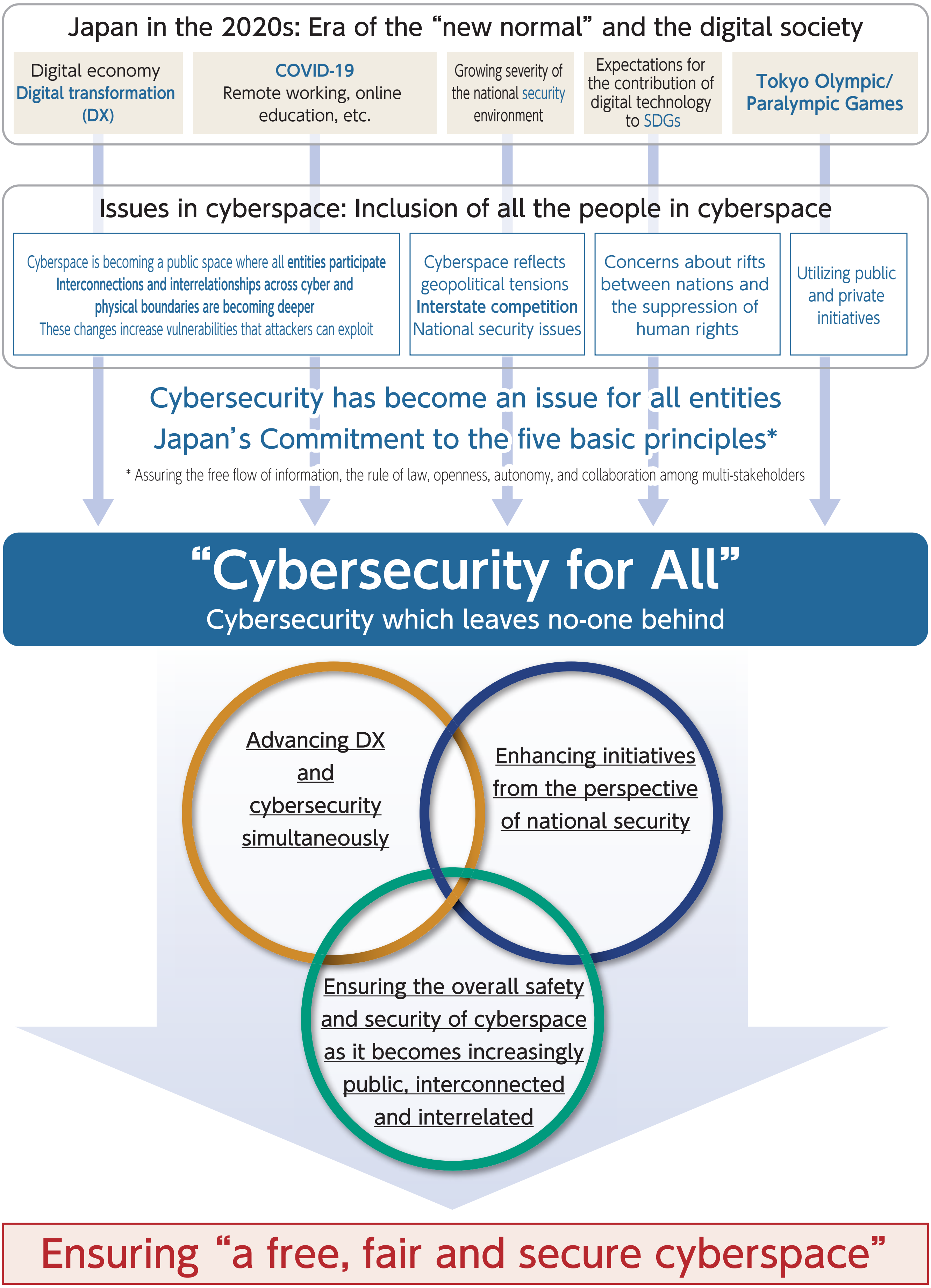
Cybersecurity which leaves no-one behind

I

Executive summary

Executive summary

Issues and Direction of Japan's Cybersecurity Strategy 2021



Japan in the 2020s: Era of the "new normal" and the digital society

- Digital economy Digital transformation (DX)
- COVID-19 Remote working, online education, etc.
- Growing severity of the national security environment
- Expectations for the contribution of digital technology to SDGs
- Tokyo Olympic/ Paralympic Games

Issues in cyberspace: Inclusion of all the people in cyberspace

- Cyberspace is becoming a public space where all **entities participate** **Interconnections and interrelationships across cyber and physical boundaries are becoming deeper** These changes increase vulnerabilities that attackers can exploit
- Cyberspace reflects geopolitical tensions **Interstate competition** National security issues
- Concerns about rifts between nations and the suppression of human rights
- Utilizing public and private initiatives

Cybersecurity has become an issue for all entities

Japan's Commitment to the five basic principles*

* Assuring the free flow of information, the rule of law, openness, autonomy, and collaboration among multi-stakeholders

"Cybersecurity for All"

Cybersecurity which leaves no-one behind

Advancing DX and cybersecurity simultaneously
Enhancing initiatives from the perspective of national security
Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

Ensuring "a free, fair and secure cyberspace"

Enhancing Socio-Economic Vitality and Sustainable Development

Issues and direction

Advancing digital transformation and cybersecurity simultaneously

- The Digital Agency was established in September 2021. This is a great opportunity to advance DX. To this end, it is important to build trust in cyberspace, which leads to participation and commitment by all the people and businesses.
- As operations, products, and services become increasingly digitalized, ensuring cybersecurity will be directly linked to corporate value.
  "Security by design" will become ever more important, and digital investments and security measures will likely become increasingly integrated.

▶ Advance cybersecurity in parallel with digitalization

Specific measures

❶ Raising executive awareness

→Visualize and incentivize initiatives based on the guidelines of cybersecurity management, and further promote such initiatives, by implementing guidelines for digital management.

❷ Advancing DX with Cybersecurity among local regions and SMEs

→Address the shortage of knowledge and human resources required for digitalization, through the development of local regions and the establishment of a registration scheme for services targeting SMEs.

❸ Building a foundation for ensuring trustworthiness of supply chains

→Advance initiatives based on the frameworks which respond to Society5.0.

▷Supply chains	: Industry-led consortium
▷Data Flow	: Definition of data management, securing the reliability of data with "trust service"
▷Security products/services	: Promotion of third-party verification services
▷Advanced technology	: Building a common foundation for collecting, accumulating, analyzing, and providing information

❹ Advancing and broadening digital/security literacy with no one left behind

→Advance initiatives which provide assistance in the use of digital technology, along with efforts to drive information education.

Realizing a Digital Society where the People can Live with a Sense of Safety and Security

Issues and direction

Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

- Cyberspace becoming **increasingly public, interconnected and interrelated, and cyberattacks becoming more organized and sophisticated.**

▶ The national government, in cooperation with various stakeholders, will take **a comprehensive and multilayered approach to cybersecurity, which is based on self-help**, mutual help and public help, and which reduces risks and increases resilience for the entire country. This will be done mainly by (1) **creating an environment where risk is managed autonomously** through self-help and mutual help, and by (2) **deploying comprehensive cyber defense** using all available means.

Specific measures (1)

Providing a cybersecurity environment which protects the people and society

❶ Ensure safety and security in cyberspace

→Establish guidelines and encourage industry-led efforts for supply chain management, and ensure safety when implementing new technologies (IoT, 5G, etc.)

→Study measures for ensuring safe and reliable telecommunications networks to protect users

❷ Cooperate with new providers of cybersecurity (accommodate cloud services)

→Create security rules for government agencies, critical infrastructure operators, etc. to consider when using cloud

→Promote cloud usage that ensures a measure of security through private-sector efforts, such as the ISMAP initiative

→Advance the development of high-quality cloud that is reliable, open and user friendly

❸ Address cybercrimes

→Actively point out criminals exploiting cyberspace or malicious business operators who provide criminal infrastructure blocking traceability for ensuring a sense of security and safety

→Strengthen police capabilities for responding to cyber incidents

❹ Deploy comprehensive cyber defense

→Enhance the functions of national CERTs/CSIRTs, which handle general coordination of integrated advancement from response to cyberattacks to policy measures, including prevention of recurrence (marshal resources and strengthen collaboration of responsible government agencies, enhance public-private partnership by working with the Cybersecurity Council and other relevant agencies and international collaboration)

→Establish an environment for comprehensive cyber defense (vulnerability handling, technical verification mechanism, and establishing functions for investigating the cause of relevant industrial control system incidents, etc.)

❺ Ensure trustworthiness of cyberspace

→Support stakeholders who possess personal information and intellectual property

→Ensure trustworthiness of IT systems and services from the perspective of economic security (government procurement, critical infrastructure, international submarine cables, etc.)

Specific measures (2)

Ensuring cybersecurity integral with digital transformation (led by the Digital Agency)

→Propose and implement the basic principle for cybersecurity in the Digital Agency' s development policy for the information systems of the national government, etc..

→Plan systems which ensure the authenticity of information and its provider, and promote their utilization. Implement the ISMAP system and encourage its use by the private sector.

Specific measures (3)

Promoting efforts by stakeholders which underpin the foundations of the economy and society

❶ Government agencies, etc.

→Advance measures based on the Common standards for Governmental Agencies and Related Agencies, and increase the overall security level of government agencies through efforts including security audits, CSIRT training and monitoring by GSOC.

→Promote the revision and implementation of the Common standards for Governmental Agencies and Related Agencies in accordance with the expanding use of cloud services and enhance the GSOC functions to enable cloud services' monitoring.

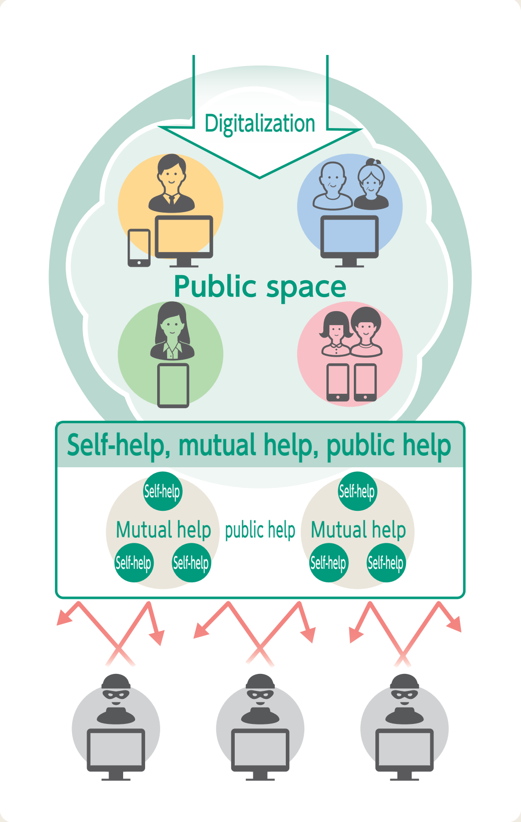
❷ Critical infrastructure

→Revise the "Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)," and advance reinforcement and management leadership in response to environmental changes.

→Update guidelines and advance efforts to establish necessary systems in response to standardization of local government information systems, handling administrative procedures online, etc.

❸ Universities, education and research institutions, etc.

→Seminars and training on risk management and incident response, supporting enhanced measures at universities, etc. possessing advanced information, including measures against supply chain risks, and so on.



Specific measures (4)

Seamless information sharing and collaboration by multiple stakeholders and enhancement of readiness to respond to massive cyberattacks, etc.

→Actively use findings and know-how obtained through response capabilities and operation at the Tokyo Games to support business operators, etc. nationwide.

→Strengthen seamless and whole of nation response capabilities, keeping in mind even in peacetime the possibility that a minor incident may escalate into a major cyberattack.

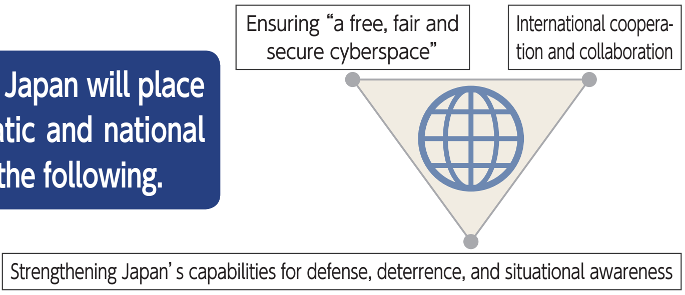
Contribution to the Peace and Stability of the International Community and Japan's National Security

Issues and direction

Enhancing initiatives from the perspective of national security

- Amidst the growing severity of the security environment surrounding Japan, cyberspace has become an realm of interstate competition that reflects geopolitical tensions. China, Russia and North Korea are presumed to be building cyber capabilities and conducting cyberattacks intended to steal information, etc..
- Meanwhile, Japan's ally and like-minded countries have been accelerating efforts to build the capabilities of their cyber commands and strengthen the ability to respond to cyberattacks, and they are collaborating to address cyber incidents and conflicts over international rules in cyberspace in particular.
- In addition, as national security has been expanding its scope to include economic and technological fields, Japan must also collaborate with its ally and like-minded countries to address conflicts over technological foundation concerning cyberspace and data, on which Japan must also establish international rules in line with its basic principles to ensure "a free, fair and secure cyberspace."

To ensure safety and security of cyberspace, Japan will place a higher priority on cyber issues in diplomatic and national security agenda, and Japan also commits to the following.


Ensuring "a free, fair and secure cyberspace"
International cooperation and collaboration
Strengthening Japan's capabilities for defense, deterrence, and situational awareness

Specific measures

❶ Ensuring a free, fair and secure cyberspace

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

▷Promote discussions on the application of international law and the practice of norms, and advance the universalization of the Convention on Cybercrime, etc.

→Formulating rules in cyberspace

▷Formulate international rules in line with Japan's basic principles, based on the progress of international efforts including Data Free Flow with Trust (DFFT), 5G security, etc.

❷ Strengthening Japan's capabilities for defense, deterrence, and situational awareness

→Increasing defense capabilities

▷Fundamentally strengthen the cyber defense capabilities of the Ministry of Defense and the Self-Defense Forces (SDF), and conduct exercises and other measures by the SDF and US military to defend infrastructure.

▷Strengthen public-private collaboration and information sharing to ensure security of advanced technology, the defense industry, etc.

→Enhancing deterrence capabilities

▷Employ capabilities to disrupt opponents' use of cyberspace for attack, use diplomatic means and criminal prosecution, and maintain and strengthen the Japan-US alliance

→Strengthening cyber situational awareness capabilities

▷Advance efforts to further clarify the actual situation of cyberattacks by leveraging the nationwide networks, technical teams and human intelligence

❸ International cooperation and collaboration

→Sharing expertise and coordinating policy

▷Strengthen multi-layered frameworks for international collaboration within and across ministries and agencies, with like-minded countries including the US, Australia, and India as well as ASEAN

→Strengthening international collaboration for incident response

▷Enhance Japan's international presence by leading international cyber exercises, etc.

→Supporting for capacity building

▷Enhance efforts in the Indo-Pacific region, including ASEAN, such as industry-academia-government collaboration, diplomacy and national security based on the Basic Policy on Cybersecurity Capacity Building for Developing Countries.

Cross-Cutting Approaches to Cybersecurity

Advance DX and cybersecurity simultaneously

Ensure the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

Enhance initiatives from the perspective of national security

Taking a cross-cutting, medium- to long-term view, promote R&D, development of human resources, and awareness-raising activities in order to advance the above.

1 Promotion of R&D

Build a government-industry-academia ecosystem, and pursue practical R&D using that as a foundation. Take medium- to long-term technological trends into consideration.

(2) Advance practical R&D

①Address supply chain risks
②Cultivate/develop domestic industries
③Foundations for monitoring, analyzing, and sharing attacks
④Advance research of cryptography, etc.

(1) Strengthen international competitiveness Build a government-industry-academia ecosystem

- Leverage measures to promote research and government-industry-academia collaboration
- Enhance research environment, etc.

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

①Advancement of AI technology
AI for Security
Security for AI

②Advancement of quantum technology
Post-quantum cryptography
Quantum communications/cryptography

2 Recruitment, development, and active use of human resources

Maintain the quality and quantity of initiatives by public and private sectors, with a focus on efforts to address environmental changes. Create an environment that enables career development spanning both public and private sectors.

(1) Advance DX with Cybersecurity

- Create an environment where people can gain additional security knowledge
- Promote practices which encourage function building and staff mobility, etc. (xSIRT, side/concurrent business, etc.)

(2) Address increasingly sophisticated and complex threats

- Strengthen human resources development programs SecHack365/CYDER/enPiT ICSCoE Core Human Resource Development Program, etc.
- Build a common foundation for human resources development and make it available to industry and academia
- Promote the use of qualification systems, etc.

Create an environment that enables talented human resources to develop careers which span the private sectors, municipalities, and national government agencies

(3) Pursue government agency initiatives

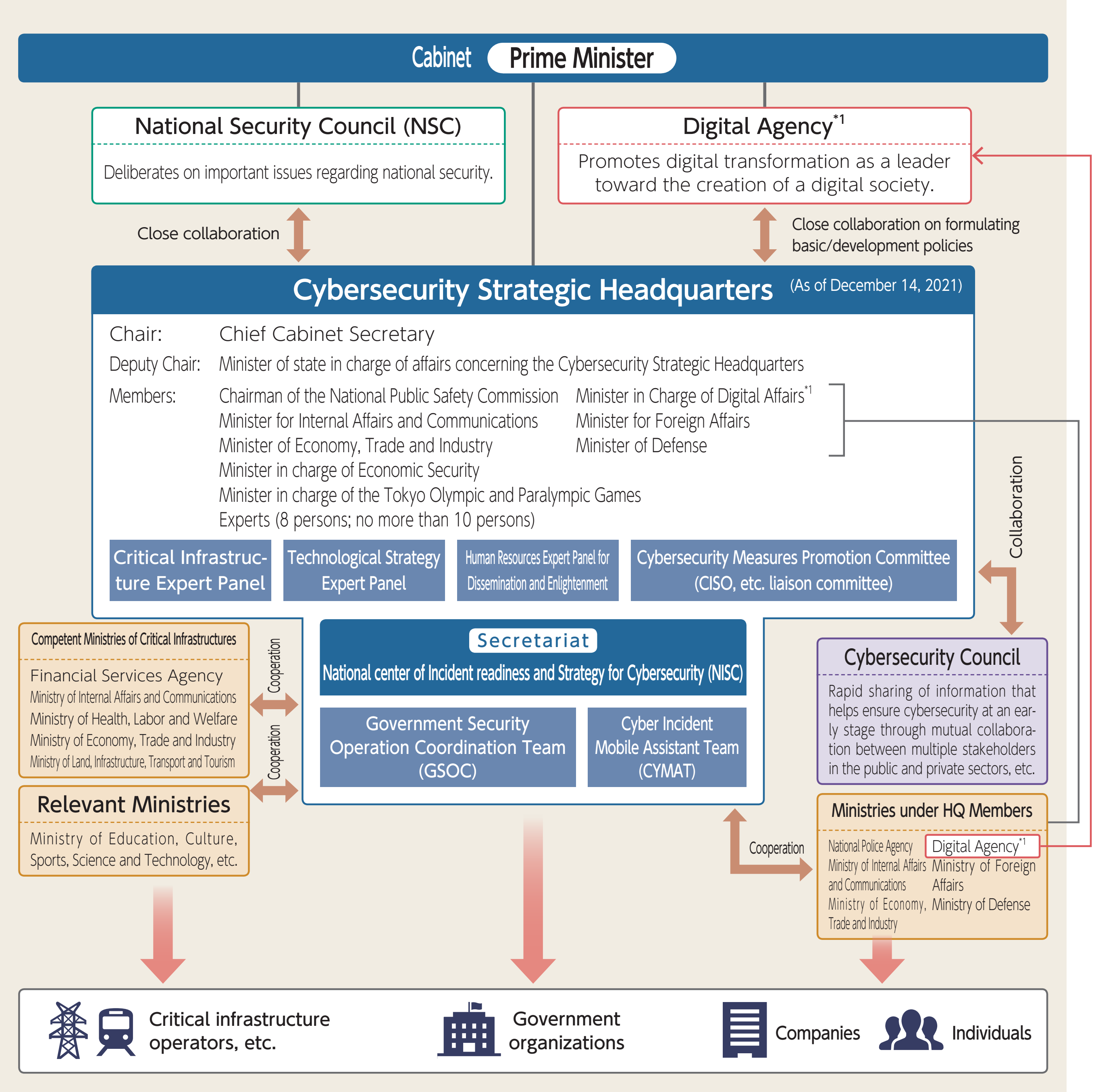
- Strengthen systems for enlisting the help of advanced outside experts
- Promote recruitment of successful candidates from the "digital division" experts
- Enhance training

3 Collaboration based on full participation and awareness raising

Improve and review action plans considering progress of digitalization, including support for the elderly.

Implementation Framework

- A concerted effort by the whole of government is needed to promote and implement cybersecurity policy in order to ensure a free, fair and secure cyberspace in line with Japan' s cybersecurity policies. Further efforts will be made to strengthen the capabilities and collaboration of relevant agencies so that they can contribute to the digital transformation led by the Digital Agency, and leverage their limited resources to fulfill their roles.
- NISC and relevant ministries and agencies must work together to actively communicate this strategy to stakeholders both in Japan and abroad, in order to encourage each stakeholder to take practical actions, and further understanding by foreign governments of Japan' s stance and enhance deterrence against attackers with the importance of international cooperation in mind.
- To enable comprehensive response by the whole of government against cyberattacks, the Cybersecurity Strategic Headquarters will improve a national CERTs/CSIRTs framework.
- Annual reports and plans should be discussed in an integrated manner, and activities for the next year aligned with the results and evaluation of the previous year' s activities, in order to develop a cohesive flow of activity which is in line with the strategy.



Cabinet Prime Minister

National Security Council (NSC)

Deliberates on important issues regarding national security.

Digital Agency[*1]

Promotes digital transformation as a leader toward the creation of a digital society.

Close collaboration

Close collaboration on formulating basic/development policies

Cybersecurity Strategic Headquarters (As of December 14, 2021)

Chair: Chief Cabinet Secretary

Deputy Chair: Minister of state in charge of affairs concerning the Cybersecurity Strategic Headquarters

Members: Chairman of the National Public Safety Commission
Minister for Internal Affairs and Communications
Minister of Economy, Trade and Industry
Minister in charge of Economic Security
Minister in charge of the Tokyo Olympic and Paralympic Games
Experts (8 persons; no more than 10 persons)

Minister in Charge of Digital Affairs[*1]
Minister for Foreign Affairs
Minister of Defense

Critical Infrastructure Expert Panel

Technological Strategy Expert Panel

Human Resources Expert Panel for Dissemination and Enlightenment

Cybersecurity Measures Promotion Committee (CISO, etc. liaison committee)

Collaboration

Competent Ministries of Critical Infrastructures

Financial Services Agency
Ministry of Internal Affairs and Communications
Ministry of Health, Labor and Welfare
Ministry of Economy, Trade and Industry
Ministry of Land, Infrastructure, Transport and Tourism

Cooperation

Relevant Ministries

Ministry of Education, Culture, Sports, Science and Technology, etc.

Cooperation

Secretariat

National center of Incident readiness and Strategy for Cybersecurity (NISC)

Government Security Operation Coordination Team (GSOC)

Cyber Incident Mobile Assistant Team (CYMAT)

Cybersecurity Council

Rapid sharing of information that helps ensure cybersecurity at an early stage through mutual collaboration between multiple stakeholders in the public and private sectors, etc.

Cooperation

Ministries under HQ Members

National Police Agency
Ministry of Internal Affairs and Communications
Ministry of Economy, Trade and Industry

Digital Agency[*1]
Ministry of Foreign Affairs
Ministry of Defense

Critical infrastructure operators, etc.

Government organizations

Companies

Individuals

(*1) Basic Act on Creation of a Digital Society (Act No. 35 of 2021), Act for Establishment of the Digital Agency (Act No. 36 of 2021). (effective since September 1, 2021)

Outline of the Cybersecurity Strategy 2021

Medium and Long Term

1 Japan in the 2020s

1-1 Establishment of the digital economy and promotion of digital transformation, expectations for contribution to SDGs, changing national security environment, impact and experience of COVID-19, and application of efforts toward the Tokyo Games.

2 Basic principles of the strategy

2-1 Ensuring a cyberspace which is "free, fair and secure"

2-2 The basic principles adhere to the 5 principles set forth in the previous strategies (assurance of the free flow of information, the rule of law, openness, autonomy, and collaboration among multiple stakeholders)

3 Issues surrounding cyberspace

Risks from the perspective of environmental changes, risks from the perspective of international affairs, and recent trends of threats in cyberspace

Strategy Period

4 Policy approaches

Three directions

(1) Advancing digital transformation and cybersecurity simultaneously
(2) Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated
(3) Enhancing initiatives from the perspective of Japan' s national security

Enhancing Socio-Economic Vitality and Sustainable Development

❶ Raising executive awareness

❷ Advancing DX with Cybersecurity among local regions and SMEs

❸ Building a foundation for ensuring trustworthiness of supply chains that support new value creation

❹ Advancing digital/security literacy with no one left behind

Realizing a Digital Society where the People can Live with a Sense of Safety and Security

❶ Providing a cybersecurity environment which protects the people and society

❷ Ensuring cybersecurity integral with digital transformation (led by the Digital Agency)

❸·❹·❺ Promoting efforts by stakeholders which underpin the foundations of the economy and society
① (Government agencies, etc.)
② (Critical infrastructure)
③ (Universities, education and research institutions, etc.)

❻ Seamless information sharing and collaboration by multiple stakeholders and application of knowledge gained through efforts toward the Tokyo Games, etc.

❼ Enhancement of readiness to respond to massive cyberattacks, etc.

Contribution to the Peace and Stability of the International Community and Japan's National Security

❶ Ensuring "a free, fair and secure cyberspace"

❷ Strengthening Japan's capabilities for defense, deterrence, and situational awareness

❸ International cooperation and collaboration

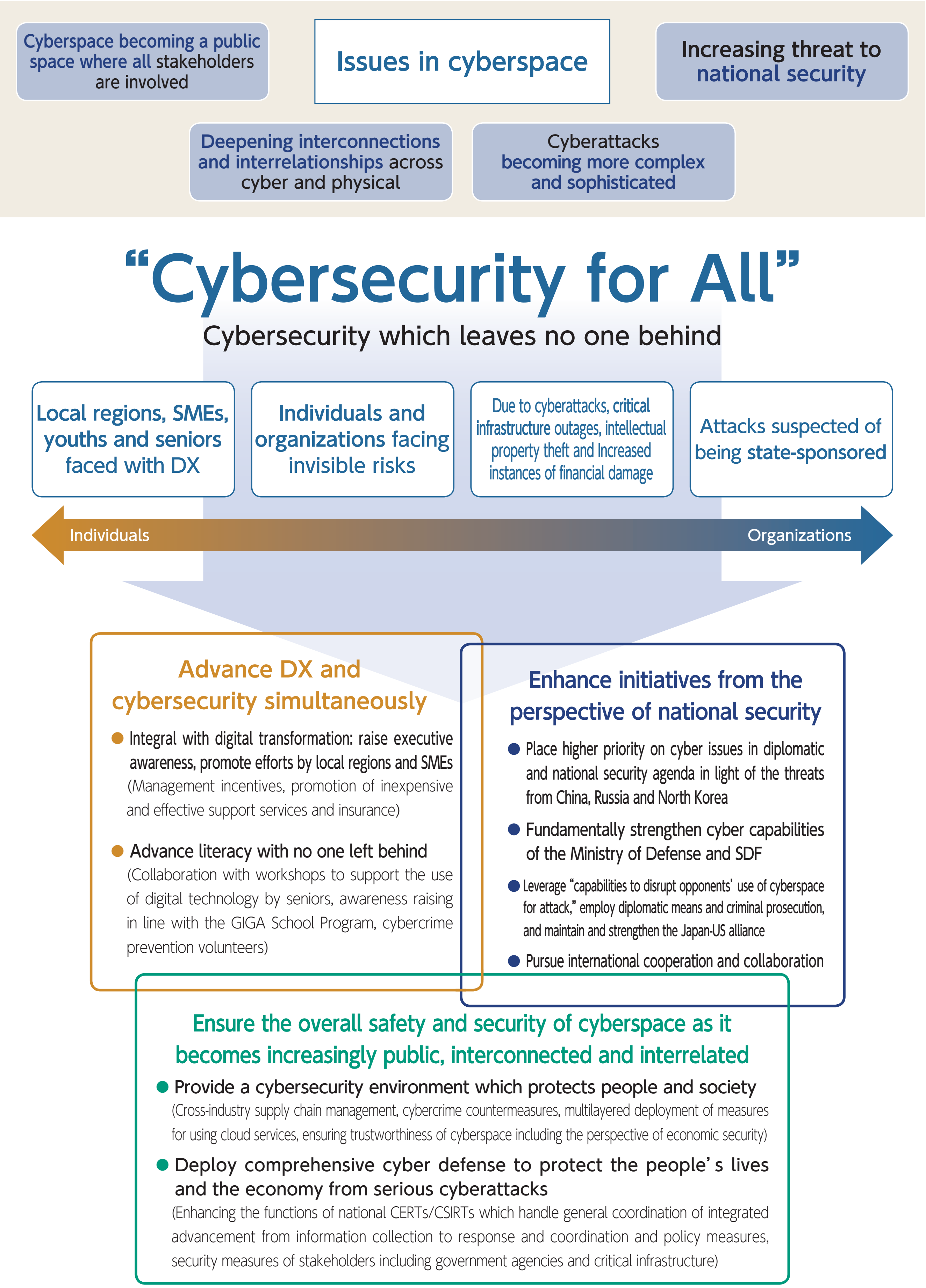
Cross-Cutting Approaches to Cybersecurity

- Promotion of R&D
- Recruitment, development, and active use of human resources
- Collaboration based on full participation and awareness raising

5 Implementation Framework

A concerted effort by the whole of government to ensure "a free, fair and secure cyberspace"

Enhancement of Efforts to Achieve “Cybersecurity for All”



Issues in cyberspace

- Cyberspace becoming a public space where all stakeholders are involved
- Increasing threat to national security
- Deepening interconnections and interrelationships across cyber and physical
- Cyberattacks becoming more complex and sophisticated

“Cybersecurity for All”

Cybersecurity which leaves no one behind

- Local regions, SMEs, youths and seniors faced with DX
- Individuals and organizations facing invisible risks
- Due to cyberattacks, critical infrastructure outages, intellectual property theft and Increased instances of financial damage
- Attacks suspected of being state-sponsored

Advance DX and cybersecurity simultaneously

- Integral with digital transformation: raise executive awareness, promote efforts by local regions and SMEs (Management incentives, promotion of inexpensive and effective support services and insurance)
- Advance literacy with no one left behind (Collaboration with workshops to support the use of digital technology by seniors, awareness raising in line with the GIGA School Program, cybercrime prevention volunteers)

Enhance initiatives from the perspective of national security

- Place higher priority on cyber issues in diplomatic and national security agenda in light of the threats from China, Russia and North Korea
- Fundamentally strengthen cyber capabilities of the Ministry of Defense and SDF
- Leverage “capabilities to disrupt opponents’ use of cyberspace for attack,” employ diplomatic means and criminal prosecution, and maintain and strengthen the Japan-US alliance
- Pursue international cooperation and collaboration

Ensure the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

- Provide a cybersecurity environment which protects people and society (Cross-industry supply chain management, cybercrime countermeasures, multilayered deployment of measures for using cloud services, ensuring trustworthiness of cyberspace including the perspective of economic security)
- Deploy comprehensive cyber defense to protect the people’s lives and the economy from serious cyberattacks (Enhancing the functions of national CERTs/CSIRTs which handle general coordination of integrated advancement from information collection to response and coordination and policy measures, security measures of stakeholders including government agencies and critical infrastructure)

Cybersecurity for All

Cybersecurity which leaves no-one behind

II

Cybersecurity Strategy

1 Introduction

In the first year of the new decade, the world was faced with a series of discontinuous changes due to the impact of the COVID-19 pandemic. As countries across the world-imposed lockdown and stay-at-home orders, it became clear that the ordinary, everyday space which provides a foundation for people's lives and economic activities was not something that can be taken for granted, but something fragile, with vulnerabilities in its various aspects. On the other hand, the effort to respond to this crisis has resulted in the accelerated use of digital technologies by the general public, and cyberspace is taking on greater importance as a sort of "public space" in our lives.

Moreover, this change can also be seen as reflecting a major trend continuing over a longer time span. The spread of digital economy continued throughout the Heisei era (1989–2019), and now in the Reiwa era, it is expected to accelerate with the Digital Agency taking the lead. While Japan is expected to contribute to the international effort to achieve SDGs[1] by 2030, the 2020s will likely be a "Digital Decade" in which the Japanese economy and society make a great leap toward the realization of Society 5.0,[2] in which cyberspace is integrated with physical space at a high level.

Meanwhile, the uncertainty surrounding cyberspace is constantly growing and changing in nature. 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. This is accompanied by the progress of information and communications technology, as well as a deepening interdependence of complex economic and social activities.

It is now clear that a "free, fair and secure cyberspace" is not a given. Rather, we are at a critical juncture where we may not be able to safeguard it. Against this backdrop, we must address the issues and challenges associated with cybersecurity with a spirit of "immutability and fluidity,"[3] an idea that constant change leads to the immutability of the value to be secured. To that end, Japan needs a new strategy, one that will serve as a cornerstone of its endeavors.

[1] Stands for Sustainable Development Goals. SDGs set out international goals to be achieved by 2030 with the aim of creating a better, more sustainable world. They were unanimously adopted by UN member states at the Summit held in September 2015 as a successor to the Millennium Development Goals (MDGs), which were formulated in 2001. SDGs, documented in the "2030 Agenda for Sustainable Development," consist of 17 goals and 169 targets, promising that "no one will be left behind."

[2] 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))

[3] This phrase is said to be the word of Matsuo Basho, a Japanese haiku poet of 17th century, who allegedly put it forward as a principle for capturing the essence of haiku. "Immutability" refers to things that transcend the passage of time and remain unchanged through the ages, and "fluidity" expresses the idea that some things change over time. These two ideas do not intrinsically conflict with each other. Rather, it is believed that true "fluidity" will naturally lead to "immutability," and true "immutability" will of itself give rise to "fluidity." (Source: *Encyclopedia Nipponica*, Shogakukan)

1.1.

Japan in the 2020s: Era of the “new normal” and the digital society

(1) Spread of digital economy and promotion of digital transformation (DX)

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. The digital economy is generating an impact that is felt in people’s lives. In Japan, the proportion of the population using the internet has exceeded 80%[4], and an average internet user now spends more than two hours a day online.[5] People’s behavior has changed, including the growing use of IoT,[6] AI, 5G,[7] and cloud services, diffusion of remote working, and implementation of ICT in education, and cyberspace is becoming a foundation of economic and social activities for everyone. This tide of change is expected to provide a positive thrust to support the realization of Society 5.0, in which cyberspace is integrated with physical space at a high level.

Meanwhile, various issues and challenges, including prevention of damage from abuse and misuse, cultivation of literacy, and measures against delays in digitalization in both public and private sectors, must be addressed appropriately in order to advance digitalization. To that end, the Digital Agency, which was established in September 2021, will lead the effort to create a digital society, and powerfully 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.”[8]

(2) Expectations for contribution to SDGs

The realization of Society 5.0, which Japan is powerfully advancing, will enable further use of data, which is expected to help solve global issues in various areas that are identified as priorities by the SDGs, including disaster prevention, climate change measures, environmental protection, and empowerment of women.

In particular, for Japan to achieve “green growth” along with “carbon neutrality in 2050,”[9] it is said that a robust digital infrastructure including smart grids and automated manufacturing is essential.[10]

(3) Changes in the national security environment

The uncertainty surrounding the existing order that Japan has enjoyed is increasing rapidly. The international community is changing at an

[4] Data from the 2020 Communications Usage Trend Survey (published on June 18, 2021) conducted by the Ministry of Internal Affairs and Communications. Internet users account for 83.4% of respondents overall, and over 50% of elderly respondents.

[5] 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.

[6] Abbreviation of Internet of Things.

[7] 5th generation mobile communication system. In September 2015, the International Telecommunication Union (ITU) issued Recommendation ITU-R M.2083, which described the key capabilities and concepts of 5G. This recommendation presented enhanced mobile broadband (eMBB), ultra-reliable and low latency communications (URLLC) and massive machine type communications (mMTC) as three scenarios for the use of 5G, listing a maximum transmission speed of 20 Gbps, a latency of about 1 millisecond, and 1 million connected devices per square kilometer as major requirements.

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

[9] In October 2020, Japan announced its aim to “achieve net zero greenhouse gas emissions, or carbon neutrality, by 2050, and become a carbon-free society.”

[10] “Green Growth Strategy Through Achieving Carbon Neutrality in 2050” (formulated on June 18, 2021)

increasing rate and is becoming more and more complicated, including the emerging competition between nations in the spheres of politics, economy, military affairs, and technology, and circumstances around cyberspace have the risk of rapidly developing into a grave situation.[11]

(4) Impact and experience of COVID-19

Faced with a series of discontinuous changes due to the impact of the COVID-19 pandemic, people were forced to respond to various restrictions and societal demands. The "new normal" lifestyle that emerged as a result partially embodied the realization of Society 5.0. Specifically, diverse work styles including remote working, implementation of ICT in education, telemedicine, and other similar initiatives advanced remarkably compared to before the pandemic.

The process of responding to the pandemic also expedited the creation and use of new services that leverage various data including personal data.[12]

(5) Application of efforts toward the Tokyo Games

The Tokyo 2020 Olympic and Paralympic Games (hereinafter referred to as the "Tokyo Games") were held in 2021. The efforts undertaken together by the public and private sectors to build response capabilities and promote risk management in preparation for this event have no doubt been an invaluable experience for Japan, including the fact that they all took place under an unprecedented environment of a COVID-19 pandemic. This experience will be applied to future events, including large-scale international events like the 2025 World Exposition (hereinafter referred to as the "Osaka Kansai Expo"), to improve Japan's cybersecurity. The knowledge and know-how acquired through these efforts are valuable for other countries as well, and they are expected to help facilitate international collaboration by being provided and shared around the world.

1.2. Meaning of the strategy

The 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 about seven years since the Basic Act was enacted in 2014.

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 above. 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 COVID-19 pandemic, digital transformation, and the experience to be gained through the handling of the Tokyo Games.

[11] See 3.2 "Risks from the perspective of international affairs" for a detailed discussion on anticipated risks.

[12] A concept that includes attribute information, travel/action/purchase histories, personal information collected from wearable devices, and human flow information, product information, and other information that are processed so that they cannot be used to identify specific individuals.

2 Concept of the strategy

Japan will adhere to its basic position on cybersecurity including the “objectives of the Basic Act,” ideas about “cyberspace to be ensured” as presented in the past two cybersecurity strategies, and “basic principles.

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 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 well-understood that the need to ensure “a free, fair and secure cyberspace” is greater than ever now when securing cyberspace is at risk.

2.2.

Basic principles

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

(1) 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 in which transmitted information reaches the intended recipient without being unfairly censored or illegally modified en route (a world where “Data Free Flow with Trust” is ensured).[13] At the same time, it must be made clear that the free flow of information does not harm the rights and interests of others without due cause, including consideration for privacy.

(2) The rule of law

As the integration of cyberspace and physical space progresses, the rule of law should be permeated in cyberspace, in the same way as in physical space as cyberspace developed as a

[13] Article 1 of the Basic Act stipulates, “ensuring the free flow of information.” Its importance is recognized internationally as well. For example, the Roadmap for Cooperation on Data Free Flow with Trust (DFFT) is endorsed in the G7 Summit Communique (June 2021).

foundation underpinning liberalism, democracy, and so forth. Similarly, it should also be made clear that any acts that threaten peace and activities that support such acts should not be condoned, assuming that existing international law including the UN Charter is applied in the cyberspace.

(3) Openness

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

(4) Autonomy

Cyberspace has developed through the autonomous initiatives of multi-stakeholders. It is inappropriate and impossible for a state to take on the entire role of maintaining order for cyberspace to sustainably develop as a space where order and creativity coexist. To maintain order in cyberspace, it is also important for various social systems to autonomously fulfill their roles and functions, thereby increasing society's resilience as a whole and deterring the activities of malicious actors, so this will be facilitated. [14]

(5) Collaboration among multi-stakeholders

Cyberspace is a multi-dimensional world established through activities of multi-stakeholders, including the national and local governments, critical infrastructure operators, cyber-related and other businesses, educational and research institutions, and individuals. For the sustainable development of cyberspace, all stakeholders are required to consciously fulfill their respective roles and responsibilities. To do so, coordination and collaboration are required in addition to individual efforts. The national government has the role of promoting this coordination and collaboration, while further promoting collaboration with other countries that share common values and cooperation with the international community, in light of changes in international affairs. [15]

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.

[14] Article 3, paragraph (2) of the Basic Act stipulates that "The cybersecurity policy must be advanced with the principle to raise awareness to each individual member of the public about cybersecurity and encourage each individual member of the public to take voluntary actions."

[15] Article 3, paragraph (1) of the Basic Act stipulates that "[cybersecurity policy] must be advanced with the principle to proactively respond to cybersecurity threats through coordination among a variety of actors."

3 Issues surrounding cyberspace

In formulating this strategy, it is important to take an approach that controls the uncertainty as much as possible, with the aim of achieving the vision of creating, through digital transformation, "a society where people can choose services that suit their needs and realize diverse forms of happiness through the use of digital technology." This must be based on an accurate understanding of not only the benefits provided by cyberspace, but also the changes and risks (including the perspectives of both threat and vulnerability) surrounding it.

Cyberspace itself has expanded quantitatively as digital services have become established in society and an increasingly diverse range of people participate in cyberspace. At the same time, its contact points with physical space have expanded to cover broader areas, and the values it can deliver have diversified qualitatively, largely through an increase in the amount of data that can be handled, the spread of new digital services through the use of IoT, AI, mobility innovation, AR/VR[16], and other cutting-edge technologies, and the establishment of the new lifestyle that has become the "new normal."

As these developments advance simultaneously, mutually affecting each other, the nature of cyberspace is changing as well. It is expected that cyberspace will become increasingly positioned as an important public space where all the 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 stakeholders across the boundaries of cyberspace and physical space are also expected to deepen further as a result of the popularization of cloud services, increased complexity of supply chains[17], and other factors.

On the other hand, the use of digital technology in cyberspace presents new challenges as well. It has been pointed out that if used inappropriately with malicious intent, it can deepen the rift and increase risks between nations, suppress human rights, and expand inequality.[18] Risks which were unforeseen previously can also be increased by the transformation of cyberspace, and changes that take place in a discontinuous manner due to the COVID-19 pandemic and other factors may generate concerns about such risks emerging in unexpected ways. While cyberspace continues to transform into a public space, it is also true that such circumstances have caused the people to continue to harbor a sense of anxiety about cyberspace.[19]

To ensure "a free, fair and secure cyberspace" with these circumstances in mind, it is necessary to clarify the issues that must be addressed and promote policies based on a proper understanding

[16] AR stands for Augmented Reality and VR stands for Virtual Reality.

[17] A supply chain generally refers to the flow of goods and information in business activities from upstream to downstream, from the receiving and placing of orders between suppliers and the procurement of materials to inventory management and product delivery. In addition, supply chains in IT may also encompass the product design stage and the operation, maintenance, and disposal of information systems and so on.

[18] This is also presented as a new challenge in the "Declaration on the commemoration of the seventy-fifth anniversary of the United Nations," (September 21, 2020) and addressing digital trust and security is considered a priority.

[19] According to a questionnaire survey conducted by the National Police Agency in September 2020, 75.3% of respondents say they feel anxious about cybercrime. (Source: "2020 Cybersecurity Policy Meeting Report" (March 2021 National Police Agency Cybersecurity Policy Meeting))

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 at the same time that these assumptions may change significantly over the medium to long term as service providers change every few years in cyberspace, which means that stakeholders that play a major role in ensuring cybersecurity can also change.

The following sections will identify the risk factors to be considered based on changes in the environment surrounding the economy and society and developments in international affairs, and show how they are emerging specifically.

3.1.

Risks from the perspective of environmental changes

While changes in the environment surrounding Japan's economy and society may provide a variety of benefits, those changes may also be accompanied by increased risks. In the following sections, those developments from the perspectives of threats and vulnerabilities of the economy and society will be mentioned.

(1) Perspective of threats

Through the use of new technologies and establishment of the so-called "new normal," new digital services continue to be created and become part of people's lives. This also means that people will be putting much more information about themselves—information that has bearing on their lives, bodies, and property—than ever before on cyberspace, both quantitatively and qualitatively. This data will be used to create sources of value and increase convenience, which benefit people. At the same time, it will provide greater incentives for attackers to carry out cyberattacks, potentially resulting in more systematic and large-scale efforts to make cyberattacks more organized and sophisticated.

As digital services begin to take root in people's lives, it is conceivable that attack methods will become more diversified and advanced, and gaps formed in the process of coordinating digital services may become vulnerabilities for attackers to target.

It is also conceivable that attackers will take advantage of the fruit of technological innovation, leading to greater threats. For example, if AI technologies are exploited by attackers, cyberattacks will be launched at a speed and on a scale beyond the level of human capabilities and technical skills. In the medium to long term, the possibility of autonomous attacks that do not rely on human control must also be taken into consideration.

(2) Perspective of vulnerabilities of the economy and society

From the perspective of the economy and society as a whole, the advancement of digitalization will inevitably involve companies in various industries and business categories that were hitherto unrelated to cyberspace, and even individuals including the young and elderly, to participate in cyberspace. While there are rising expectations 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 in the economy and society through the misuse of devices and services.

In addition, we are seeing increased use of cloud services, expansion and widespread adoption of products and services delivered through complex global supply chains, greater use of IoT devices among industries (i.e., everything becomes connected to networks), and application of AI technology to various systems. Due to these developments, 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 remote working becoming an established part of business operations, is revealing the limitations of the traditional concept of “perimeter security.”[20]

3.2.

Risks from the perspective of international affairs

As cyberspace has become a realm of interstate competition that reflects geopolitical tensions even during normal times, and due to the 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 such, the situation in cyberspace, while not amounting to national emergency per se, can no longer be deemed purely in peacetime.

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, evolving into an issue of national security. Attackers 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 is also presumed to conduct 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.[21]

In addition, as differences in basic values become apparent and 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 underpins 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

[20] This concept is based on the idea of establishing a perimeter and cutting off the inside from the outside to prevent attacks from the outside and information leakage from the inside. Perimeter security assumes that “things that cannot be trusted” do not enter through the perimeter, and only “things that can be trusted” exist inside. This security model is mainly intended to defend networks.

[21] Specific trends are detailed in 4.3 Contribution to the Peace and Stability of the International Community and Japan’s National Security.

complex and globalized, the risk of malicious functions, etc. getting embedded in products 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 the threat of cyberattacks, 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.

3.3. Recent trends of threats in cyberspace

Risk factors discussed above are seen as clear trends from observing the recent stream of threats in cyberspace.

Many attacks suspected of involvement of crime organizations or states are taking place. Overseas, attacks interfering with democratic processes including those targeting elections, large-scale attacks exploiting vulnerabilities in supply chains, attacks targeting industrial control systems, and other attacks against infrastructure that could impact a wide range of economic and social activities as well as national security 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[22] 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 (e.g., business email compromise and phishing attacks related to vaccination news), attacks via overseas branches where countermeasures tend to be relatively difficult to reach, and attacks carried out through highly anonymous infrastructure.

In addition, Advanced Persistent Threat groups 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 demand money in return for restoring data and stopping the disclosure of stolen data,[23] and the misuse of anonymization and encryption technologies by attackers to avoid being tracked. 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 as well as national security by halting production activities, causing service disruption, doing financial damage, and stealing personal and confidential information.

[22] An abbreviation for Virtual Private Network. It refers to the technology or device used to simulate a situation where private networks are connected by a dedicated line via the internet or a closed network used by a large number of people, using encryption and traffic control technologies.

[23] For example, the G7 Summit Communique (June 2021) refers to "the escalating shared threat from criminal ransomware networks."

4 Policy approaches toward achieving the objectives – Cybersecurity for All

In this section, targets and guidelines of the policies to be implemented in the coming three years will be presented, based on the understanding of issues discussed in the preceding sections, with the aim of achieving the objectives set forth in the Basic Act.

As stated above, cyberspace itself has both expanded in quantity and evolved in quality, becoming increasingly integrated with the physical 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 regions, etc. 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 "with 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 three directions stated below.

These directions each correspond primarily to the efforts toward "enhancing socio-economic vitality and sustainable development," "realizing a digital society where the 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," as discussed in this section. In light of an understanding of issues discussed up to the preceding section, these directions must be kept in mind in implementing measures to achieve any of these objectives.

<Three directions>

(1) Advancing digital transformation (DX)[24] and cybersecurity simultaneously

The COVID-19 pandemic has had the effect of advancing the establishment of the new normal, and the Digital Agency was established in September 2021 to lead the effort to create a digital society. Given these circumstances surrounding the digitalization of the economy and society, it is undeniable that now is an excellent time to make up for Japan's delay in digitalization.

On the other hand, unless awareness of cybersecurity is raised and trust is built in the technological foundation and data that compose cyberspace, active 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 business transformation. Conversely, properly addressing risks that change along with digitalization may also lead to increased awareness and trust regarding cybersecurity.

Digitalization has a strong connection with ensuring cybersecurity from the perspective of not only the economy and society as a whole but also the activities of individual companies. It is expected that the ability to respond to IT systems

[24] Digital transformation is typically abbreviated as DX. The "DX Report" issued in September 2018 (Study Group for Digital Transformation of the Ministry of Economy, Trade and Industry) cites the following definition: "An effort by companies to create value and establish competitive advantage by transforming both online and real customer experience through new products and services and new business models, utilizing the third platform (the cloud, mobility, big data/analytics, social technology), responding to disruptive changes in external ecosystems (customers, markets), and driving transformation of internal ecosystems (organizations, cultures, employees)."

and digitalization will form 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, in both micro and macro perspectives, it is important to promote digitalization along with efforts to ensure cybersecurity (hereinafter referred to as "DX with Cybersecurity"). All stakeholders must pursue their initiatives with this understanding. In the current efforts toward digital transformation, the groundwork has just been laid for advancing digital transformation and cybersecurity at the same time, with the Basic Act on the Formation of a Digital Society (Act No.35 of 2021) clearly stipulating that cybersecurity must be ensured. The national government will powerfully support all efforts aimed at digitalization, including the creation of an underlying foundation.

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

In the previous cybersecurity strategy formulated in 2018, 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 in the economy and society, 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 the approaches (deepen mission assurance and enhance efforts related to risk management) without overlooking the asymmetrical situation with the attackers, and work to improve the environment and address the causes.

Such societal demands require all stakeholders involved in cyberspace to assume greater roles. While the importance of independent efforts ("self-help") and close coordination among multiple stakeholders ("mutual help") remains unchanged, 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. In doing so, the national government will strengthen the framework of national CERTs/CSIRTs[25] while ensuring they can fulfill their function by making improvements and enhancements based on follow-up. National CERTs/CSIRTs are responsible for general coordination to enable response to

[25] Generally, CSIRT is an abbreviation for Computer Security Incident Response Team. It is an organization that monitors for security problems in information systems, etc. within companies, government agencies, and other entities. In the event of a problem, it analyzes the cause and investigates the scope of impact. CERT is an abbreviation for Computer Emergency Response Team. It is an organization that responds to computer security incidents. In Japan, when cyberattacks are addressed through international collaboration, specialized government and private sector organizations work together to respond. In this strategy, national CERTs/CSIRTs are positioned as "a function responsible for general coordination in the event of a serious cyberattack to enable a series of actions ranging from information collection and analysis to investigation, evaluation, issuing alerts, responding to the attack, and subsequent planning of policy measures to prevent recurrence, etc., to be pursued in an integrated manner" (see 4.2.1(4) for details).

incidents that cannot be handled through self-help or mutual help, as well as subsequent policy measures to prevent recurrence and make improvements, to be pursued in an integrated manner.

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

Previously, the idea of "mission assurance"[26] 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 services through cyberspace. With many stakeholders involved 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. The impact of incidents is also becoming more widespread and complex, and it is becoming increasingly difficult to foresee the repercussions and resolve the incidents. Taking cloud services as an example, the impact may now extent not only to businesses that use a certain cloud service, but also to the end users who use the services of those 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. Based on this understanding, entities that use cyberspace to perform operations or provide services are required to take the entire supply chain into consideration, not just the one-to-one relationship between the providers and users, and act responsibly with the reliability of the supply chain in mind.

The importance of the concept of "mission assurance" should remain unchanged. 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 supply chain, from the operations that they must perform and products and services that they must provide 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 and efficiently (through the use of automation technology, etc.) defend against cyberattacks while making efforts to constantly review anticipated risks and ensuring the possibility of tracking attacks (hereinafter referred to as "traceability") after they occur, in light of the trend of threats.

Cyberspace is used as a key channel for stealing personal information, information concerning intellectual property, which is a source of international competitiveness, and information related to national security. Given this situation,

[26] Refers to the condition in which any organization represented by companies, critical infrastructure operators, and government bodies understand the operations or services that they should carry out as their missions, and ensure necessary capabilities and resources to reliably execute such missions. This means that senior executives or managers of each organization should identify operations or services that represent their missions and take all responsibility for secure and sustainable provision, rather than making cybersecurity initiatives themselves the goal.

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 Ministry of Defense and the Self-Defense Forces (SDF), 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 its 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 its 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.

4.1.

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.

It is vital that the perspective of cybersecurity is incorporated and measures are advanced for all initiatives in the course of promoting the digitalization of the economy and society—raising executive awareness, implementing initiatives directed toward local regions and SMEs, building a foundation for the entire cyberspace as it becomes increasingly public, interconnected, and interrelated in the digital age, and improving the literacy of all members of the economy and society.

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, etc. 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. Based on this understanding, it is necessary to raise executive awareness and advance initiatives pursued by companies to strengthen cybersecurity in line with digitalization.

To advance digital management, matters that business managers are expected to practice to improve corporate value have been summarized as digital management guidelines, and business managers are encouraged to implement them, from the perspective of creating an environment where funds, talent, and business opportunities flow toward companies that autonomously pursue digital transformation.

Moreover, to strengthen cybersecurity, the government will build on previous efforts to raise awareness about guidelines that illuminate the importance of advancing security measures under the leadership of management. This will be done by continuing to promote their use through guidance and examples provided to facilitate their implementation, and updating them as necessary.

With this understanding, the government will work to ensure that efforts to strengthen cybersecurity in line with digitalization are visualized so that investors and other stakeholders who value sustainability will be aware of them, and that incentives are generated for such efforts. It is expected that this will lead to a general recognition—from both inside and outside companies, including markets—of companies' efforts as contributing to a sustainable improvement of corporate value, fostering a momentum to promote further efforts. Specifically, cybersecurity initiatives will be positioned in policies to promote digitalization, including tax measures for digital-related investments and the selection and announcement of forward-looking companies that practice digital management guidelines and work on digitalization. In addition, the use of tools and guidelines to visualize the status of initiatives to stakeholders in and outside companies will be advanced. Through such efforts, the government will follow up on the status of corporate initiatives when the promotion of practices such as ascertaining cybersecurity risks by executives and the disclosure of corporate information is expected.

Moreover, the government assumes that communication with experts in and outside companies will be indispensable for executives who pursue cybersecurity measures along with digitalization through such integrated advancement measures as those stated above to appropriately identify the risks inherent in the digital services that are the source of their company’s competitive strength. To this end, the government will push forward with efforts to create an environment where executives can gain additional knowledge as needed even when they may not necessarily have expertise or work experience related to IT or security, when such knowledge becomes necessary in collaborating with internal and external security experts (hereinafter referred to as “‘Plus Security’ knowledge”). [27]

4.1.2 Promotion of “DX with Cybersecurity” among local regions 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 are expected to spread to local regions, SMEs, and various industries and business categories that were previously unrelated to cyberspace, without exception.

On the other hand, SMEs face a lack of expertise, talent, and other resources in their effort to pursue cybersecurity measures along with digitalization due to a difficulty deploying staff specialized in security. These are issues that must be addressed.

Therefore, in building local communities based on the idea of mutual help, the government will continue to develop their functions and promote efforts to create opportunities for local regions faced with a lack of resources to address issues and generate added value. The government will do this not only through consultation with experts but also by matching businesses and human resources, nurturing talent, and developing regional security solutions. Leading practices will also be shared to help roll out these activities across Japan.

For SMEs, it is difficult to allocate a large budget to security. To address this issue, security measures targeting SMEs will be advanced, including making inexpensive, effective, and accessible security services and insurance products widely available for SMEs. Specifically, the government will advance efforts including review and registration of services that meet certain criteria for granting trademark usage rights, and self-declaration of security measures, in cooperation with an industry-led consortium established with the aim of enhancing the cybersecurity of entire supply chains, including SMEs. The government will also create incentives by making self-declaration a requirement for subsidies targeting SMEs. It is expected that these initiatives will help visualize efforts to strengthen cybersecurity for business partners, etc., creating an opportunity to expand initiatives to cover local regions and SMEs.

In addition, the government assumes 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

[27] Specific measures for creating an environment where non-executives can also gain “Plus Security” knowledge will be discussed in detail in 4.4.2 (1) (i).

due to the placement of information assets off company premises, as well as problems with settings, etc. Accordingly, the government will communicate guidance and other matters that cloud service users must keep in mind, and consider ways to urge cloud service providers to offer necessary support, including the provision of information and tools to the users, to prevent or reduce configuration errors when using cloud services.

4.1.3 Building a foundation for ensuring trustworthiness of supply chains that support new value creation

It is expected that all stakeholders will create new value by freely establishing interconnections and interrelationships toward the realization of Society 5.0, in which cyberspace is integrated with real space at a high level. On the other hand, from the perspective of ensuring its trustworthiness, it will be necessary to respond appropriately to issues that arise under such newly established interconnections and interrelationships.

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, the government will advance initiatives to ensure cybersecurity that will serve as a foundation for building trustworthiness in supply chains supporting new value creation in Japan.

(1) Ensuring trustworthiness of 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 assumed that risk management with a view of entire supply chains will become increasingly important.

With this understanding, the government will promote efforts to develop and implement concrete security measures in the industry by formulating both industry-specific and cross-industry guidelines and promoting their use based on the above frameworks, etc.

The government will also assist efforts made by a consortium that engages in awareness raising and developing concrete initiatives with the aim of strengthening cybersecurity measures across supply chains, joined by organizations from various industries. Under this framework, it is expected that the government expands its activities to cover local regions and SMEs through supply chains, and increase the trustworthiness of entire 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) Ensuring trustworthiness of 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).[28]

Based on the characteristics of data whose attributes keep changing as it flows between different stakeholders, the government will work to clarify the definition of data management and establish frameworks including procedures for identifying risks and use cases, from the perspective of identifying risk points. The government will use

[28] 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)

these frameworks to ascertain gaps between the rules of each country that handles data distributed across national borders.

It is also necessary to create an effective mechanism for preventing spoofing of sources, falsification of data, etc. (hereinafter referred to as “trust service”) to make it available for use. With respect to the reliability of trust service, which ensure and prove the authenticity and integrity of elements such as stakeholders, intentions, facts, information, presence, and time, the government 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) Ensuring trustworthiness of security products and services

For independent efforts aimed at cybersecurity to spread, security products and services provided in the market must be trustworthy. As concerns about supply chain risks grow, and it becomes increasingly difficult for the developers themselves to identify risks in entire systems due to common use of open API[29] and OSS[30], it is believed that demand will grow for objective third-party verification and evaluation from the perspective of demonstrating the reliability of company products, etc. both internally and externally, and businesses that meet such demand will become even more important as an industry. From these perspectives, the government will work to build a foundation for ensuring reliability and, coupled with efforts related to the practical application of advanced technology and innovation, nurture products and services made in Japan without relying excessively on other countries.

Specifically, the government will promote business matching by establishing a foundation for verifying the effectiveness of security products and services and by performing verification tests in production environments. In addition, the government will review, register, and list up security services that meet certain standards and promote the use of such services by government agencies. The national government will also discuss efforts to visualize the reliability of verification service providers toward the creation of a verification business market.

(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. The government must respond to the demand from society by urgently advancing the establishment of a government-industry-academia ecosystem that facilitates active industry-academia collaboration, and by encouraging open innovation activities.

Security products and services 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 its effort to break through this situation, the government will build an intellectual

[29] API, which is an abbreviation for Application Programming Interface, is an input and output mechanism that one software makes available to another software.

[30] OSS, which is an abbreviation for Open Source Software, collectively refers to software whose source code can be used, investigated, reused, modified, expanded, and redistributed, regardless of the purpose of the user.

foundation for collecting, accumulating, analyzing, and providing cybersecurity information within the country, and while being mindful of information management from the perspective of national security, the government will share such information effectively with various stakeholders as a node for industry, academia and the government. In doing so, the government will actively share opinions with stakeholders and form communities so that it will be useful for the government, industry, and academia in R&D and product development.

In addition, the government 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 its effort toward the practical application of these new technologies, the government will promote technical reviews aimed at the use of new technologies in government agencies. In addition, to facilitate the global expansion of security products and services made in Japan, the government will continue to advance initiatives toward international standardization and support for exhibiting at overseas trade shows.

4.1.4 Advancing digital/security literacy with no one left behind

The foundation of cyberspace is becoming a basic infrastructure for people’s lives. As we pursue “people-friendly digitalization, with no one left behind”[31] in this context, it is essential that each of the people acquire skills and basic knowledge and ability (i.e., literacy) in cybersecurity so that they can use their own judgment to protect themselves from threats and enjoy its benefits.

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 Individual Number Card, and implement the GIGA School Program,[32] it is more important than anything to encourage ourselves to actively try using them and gain experience toward enhancing and establishing literacy. At the same time, various initiatives to accompany efforts to advance information education should be implemented.

The government will work 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 that leverage opportunities for such uses. For example, the government will raise awareness about matters requiring attention concerning cybersecurity through collaboration with mobile phone dealers and other local stakeholders for efforts targeting the elderly, and with elementary schools, junior high schools, and cybercrime prevention volunteers for efforts targeting children. As for the advancement of the GIGA School Program, the government will deploy assistants who will help teachers with their daily use of ICT, enhance the ability to provide guidance on the use of ICT in teacher-training programs, prime students when introducing computers, and advance education on information ethics using video materials, etc.

With regard to the spread of disinformation on the internet, the government 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.

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

[32] This program seeks to provide one computer for every student and broadband communication networks to schools.

4.2. Realizing a digital society where the people can live with a sense of safety and security

Now that cyberspace is taking on an increasingly public nature, and deeper interconnections and interrelationships are forming across cyber and physical boundaries, providers of all services are required to take the idea of “mission assurance” a step further and practice risk management in keeping with such changes in cyberspace. The security of cyberspace must be ensured to enable all the people and stakeholders involved in cyberspace to participate in it with peace of mind. To that end, the national government will take a comprehensive approach to cybersecurity and work in cooperation with relevant stakeholders to create an environment where autonomous risk management is practiced through self-help and mutual help. For the socio-economic infrastructure that serves as the foundation of the people’s safety and security, the government will also lead implementation for the whole society by actively introducing advanced initiatives while using all means available to implement comprehensive cyber defense. This will be done while constantly reviewing its defensive measures and the key assets subject to defense against cyberattacks, and collaborating with relevant stakeholders, with the aim of ensuring the safety and trustworthiness of cyberspace.

Through these initiatives, the government will achieve a multi-layered cyber defense that is based on the self-help, mutual help, and public help of all stakeholders involved in cyberspace, which reduces risks and increases resilience for the entire country.

4.2.1 Providing a cybersecurity environment which protects the people and society

Given the increasingly public nature of cyberspace, it is necessary to realize a society where all stakeholders can enjoy convenience and cybersecurity. The national government will collaborate with relevant stakeholders in this effort, working to visualize the technological foundation and services that make up cyberspace and improve traceability in the event of an incident. These improvements will foster an environment where each stakeholder can choose appropriate risk management options suited to their needs. In addition, by securing traceability and encouraging victims of cybercrimes to report to the police and notify public agencies, the national government will eliminate factors and environments that tolerate cybercrimes. These initiatives will be pursued based on the principle of “assurance of the free flow of information.”

With such changes taking place in cyberspace, the impact of incidents is becoming increasingly complex and may spread over a wide area. As such risks come to the fore, the government will work with relevant stakeholders to create an environment where it is standard practice for service providers to take a comprehensive view of the interconnections and interrelationships across cyberspace as they seek to thoroughly manage risks, 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 actively work together with relevant agencies, take the attackers' viewpoints into account as well, and use all means available to implement comprehensive cyber defense, thereby working energetically to reduce risks and increase resilience for the entire country.

It is also vital for the national government to constantly review the key assets subject to defense against cyberattacks. In addition to information related to national security, 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, the government will work to increase the traceability and visibility of cyberspace through an integrated approach that encompasses both public and private sectors. These initiatives will be pursued based on the principle of "assurance of the free flow of information."

(i) Establishing supply chain management grounded in cybersecurity

To undertake necessary supply chain measures that include risk management, 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 stakeholder with a broad view of the entire supply chain, including SMEs, overseas offices, and business partners.

In addition, the national government will build a mechanism for securing the reliability of supply chain components including devices, software, data, and services. In addition, the national government 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 trustworthiness 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, the government 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, the government 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 the government will advance the use of a framework that meets the requirements for such a combination of safety and security.

The government will also 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.

Moreover, the government will ensure safety and security by formulating guidelines and codes of conduct for cybersecurity in new fields, including autonomous driving, drones, automated factories, smart cities,[33] crypto assets,[34] and the space industry.

(iii) Ensuring safety and security to protect users

From the perspective of enabling secure use of telecommunications services and activities in cyberspace, the government will study measures for ensuring safe and reliable telecommunications networks while adjusting relevant laws and regulations as necessary.

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

(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.

Cloud services in particular have become an essential infrastructure in cyberspace, but users are also faced with unintended incidents due to misconfiguration of services, for example. These incidents may in some cases be hard to recognize or impossible to resolve alone. Also, in cloud services the same incident may affect multiple users at the same time. In light of these circumstances, the government will push forward with the establishment of an open, high-quality cloud that is reliable and easy to use, so that users will be able to entrust their information assets to cloud services with peace of mind. The government will also work with the users, cloud service providers, system contractors, and other stakeholders to formulate cybersecurity rules that should be considered in the process of designing and developing information systems for government agencies, critical infrastructure operators, and others to use cloud services. This will enable users to select appropriate cloud services that meet their risk management guidelines, and correctly understand security policies and responsibilities, while fostering a relationship with service providers in which any difference of understanding can be properly

[33] Smart cities are sustainable cities and communities where various issues faced by traditional cities and communities are resolved and new value continues to be created through the use of ICT and other new technologies, along with a wide range of private and public sector data. These technologies and data are used to provide services that are tailored to each individual, and realize sophisticated management (e.g., planning, maintenance, control, and operation) in various fields. Smart cities are places where Society 5.0 is realized ahead of the rest of the country.

[34] Crypto assets are neither legal tender nor assets denominated in legal tender, but they can be used for the payment of compensation to unspecified persons or exchanged with legal tender in transactions with unspecified persons, as well as being electronically recorded and transferred.

addressed. At the same time, the government will implement initiatives to visualize the safety of cloud services using ISMAP[35] and other means. These efforts will target a wide range of stakeholders in both public and private sectors and promote increased use of cloud services that ensure a certain level of security. As many cloud services are provided by foreign companies, Japan will work to advance global collaboration as well.

These measures will be implemented in a multi-layered approach, and offered in a package as necessary, to ensure cybersecurity for SMEs and users in local regions, building a safe and secure cloud service usage environment across Japan.

(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.

To be able to deal with crime committed by misusing crypto assets, the dark web, social media, and so on, and crime that makes use of advanced information and communication technologies, the government will strengthen its investigative capabilities and technological prowess, and advance comprehensive analysis for predicting threats to cyberspace and for unraveling those threats technologically.

The 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. In addition, the government will advance countermeasures against cybercrime in which public and private sectors collaborate each other in information sharing and analysis, prevention of damage due to cybercrime, and human resource development. To prevent damage from cybercrime by encouraging each individual to take voluntary measures, the government will collaborate with related institutions and organizations, including volunteer groups engaged in cybercrime prevention, and advance public awareness campaigns.

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

In addition to these initiatives, the government will also strengthen efforts such as cooperation with relevant business operators and international collaboration, drawing on efforts made by other countries, in order to remove environments and causes that tolerate the current asymmetric situation with attackers. Regarding the appropriate preservation of communications history data logs in particular, the government, on the basis of the relevant guidelines, will get related business operators to take appropriate measures.

To ensure these efforts are implemented effectively, the government will strengthen the

[35] Abbreviation of Information system Security Management and Assessment Program. ISMAP has been in use since FY2020 to assess the security management of government information systems.

ability to respond to cyberattacks, for example, by considering creating dedicated operational units and a function for leading cyber departments within police organizations.

(4) Deploying comprehensive cyber defense

As for serious cyberattacks that undermine the people's safety and security by disrupting critical infrastructure services and stealing personal information, intellectual property, and money, there is a limit to the response that can be made through individual stakeholders through self-help and mutual help, given the deepening interconnections and interrelationships in cyberspace. It is also difficult to assess the overall impact of such cyberattacks, making it increasingly challenging to implement effective defense.

For these reasons, the government will respond to such serious cyberattacks as a nationwide effort. Working in collaboration with relevant stakeholders and using all means and capabilities available, the government will implement comprehensive cyber defense measures that advance incident response ranging from obtaining and analyzing appropriate information as needed to dealing with specific cases, and policy measures including creating rules to prevent recurrence and make improvements.

(i) Strengthening the function of national CERTs/CSIRTs that are responsible for general coordination of comprehensive cyber defense

The government will reinforce the framework of national CERTs/CSIRTs as a function responsible for general coordination in the event of a serious cyberattack to enable a series of actions ranging from information collection and analysis to investigation, evaluation, issuing alerts, responding to the attack, and subsequent planning of policy measures to prevent recurrence, etc., to be pursued in an integrated manner. Specifically, the government will improve response capabilities and enable integrated and coordinated response by marshalling resources and strengthening collaboration of responsible government agencies. The government will also strengthen collaboration with cyber-related enterprises to expedite response and coordination, including collecting information about cases whose impact may spread across different organizations and sectors, and initial response. The government will streamline public-private and interstate information sharing, response, and coordination by further advancing collaboration between information sharing systems and with relevant overseas agencies. These include the Cybersecurity Council,[36] Cybersecurity Response and Coordination Center,[37] and specialized agencies that have sufficient technical capabilities and expertise in communication and coordination with stakeholders in and outside Japan. Moreover, the government will carry out general coordination with public and private stakeholders in light of issues presented by incidents and insights obtained as a result. The national government will also formulate policies and implement measures as necessary and in a timely manner, including establishment of systems.

[36] The Cybersecurity Council was organized on April 1, 2019 based on the Act Partially Amending the Basic Act on Cybersecurity (Act No. 91 of 2018), which was enacted in December 2018, to enable mutual collaboration between various public and private stakeholders and discussion on how to advance cybersecurity measures. The Council operates with the aim of preventing and containing damage from cyberattacks by enabling various stakeholders, both public and private and regardless of the industry, to collaborate effectively and quickly share information needed to ensure cybersecurity.

[37] The Cybersecurity Response and Coordination Center collects threat and incident information concerning cybersecurity for the Tokyo Games, provides that information to relevant agencies, and supports and coordinates incident response by relevant agencies. It was established on April 1, 2019. It will be closed at the end of March, 2022.

Through these efforts, the government will enable rapid information collection as needed from public and private stakeholders, and strengthen the ability to quickly assess the overall picture of damage. With the aim of improving Japan' comprehensive defense capabilities, the government will further advance the following: provision of timely alerts and information tailored to various management and frontline needs, which contribute to greater impact and coverage of information provided concerning national defense, and more effective defense and systematic, detailed response according to the nature and severity of the attack and circumstances of each sector; cooperation with global operations seeking to render cyberattacks harmless; and quick formulation of policy through seamless general coordination.

(ii) Establishing an environment for steady implementation of comprehensive cyber defense

The government will work together and discuss measures concerning "Active Cyber Defense"[38] including vulnerability handling, technical verification mechanism for verifying the reliability and security of IT systems and services, 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.

Also, given that incidents attributable to IT systems implemented as part of the foundation underpinning Japan's socio-economic activities and the lives of its people may lead to the suspension of its functions, the government will assess vulnerabilities in cyberspace that may jeopardize the autonomy of missions and functions, and consider actions to ensure its trustworthiness, from the perspective of economic security.

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

The government will seek thorough implementation of countermeasures by providing timely and appropriate information about effective safety management measures that protect personal information from cyberattacks.

The government will also strengthen efforts in cooperation with relevant organizations to promote the sharing of information that contributes to security measures 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 government will advance measures including study of systems to ensure the security and trustworthiness of IT systems and services that are embedded in critical socio-economic infrastructure with a major impact on its people's lives and economic and social activities, as well as their mode of business alliance and service contracts, examining various risk scenarios including supply chain risks as well. The government will also advance the development of

[38] Active Cyber Defense involves cooperating with cyber-related enterprises and implementing active preventive measures against threats in advance.

new technologies needed to this end.

The government will advance the protection of international submarine cables and other infrastructure on which Japan depends for a majority of its communication with overseas, and ensure their security, trustworthiness, and redundancy, through international and public-private collaboration.

The government will advance efforts to create international standards for IT devices and services, and pursue international collaboration including standardization and establishing technical verification mechanism to ensure security and trustworthiness. In particular, the government will enhance trustworthiness of IT systems and services from the perspective of both system and technology. The government will do so by strengthening efforts including supply chains for procuring government information systems and advancing the use of a security assessment system (ISMAP), and by initiating efforts to establish technical verification capabilities and create necessary standards.

4.2.2 Ensuring cybersecurity integral 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 (hereinafter referred to as “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 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[39] 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

[39] Abbreviation of Government Security Operation Coordination team. The GSOC team operates the GSOC system designed for cross-government monitoring through sensors installed in each agency, analyzing attacks, providing advice to each agency, promoting mutual collaboration between agencies, and information sharing. The first GSOC team was launched in April 2008 to monitor government agencies, and the second GSOC team started operation in April 2017 to monitor incorporated administrative agencies.

the Digital Agency on its own or jointly with each ministry, ensuring stable and continuous operation including security.

In addition, 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 and address incidents 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 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,"[40] the national government will promote the revision and implementation of the Common standards for Governmental Agencies and Related Agencies[41] in accordance with the expanding use of cloud services and consider enhancing the GSOC functions to enable cloud services' monitoring.

The 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 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 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)

Japan'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

[40] This principle summarizes the basic concept of cloud-by-default in government information systems, with the users of cloud services as the first candidate.

[41] This is a unified framework for improving the level of information security of government agencies and incorporated administrative agencies. It sets a baseline for their information security and specifies matters that need to be addressed to further raise the level of security.

infrastructure, which is subjected to threats that increase year after year, and enhancing its resilience.

The Basic Act 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, the government will ensure the stakeholders involved in critical infrastructure understand their responsibilities, and the government 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 the 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 the national government continues 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, the national government will base its efforts on the current "The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)"[42] 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, the national government 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, the national government 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. The national government 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

[42] The national government have formulated and advanced 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, as a basic framework for critical infrastructure protection. This policy revises the 3rd Edition based on the idea of functional assurance that aims to provide secure and sustainable services with an eye to the rapidly heightening threat of cyberattacks in recent years and the Tokyo Games.

information, and provide basic services closely related to the 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 the national and local governments.

To ensure security measures are steadily implemented based on the "Guidelines for information security policy for local governments,"[43] the national government will support initiatives aimed at securing and training human resources, enhancing systems, and securing necessary budgets.

The national government will continue to update the Guidelines 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."[44]

With regard to the Social Security and Tax Number System, which closely relates to the people's lives and personal information, the national government 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.

To this end, the national government will initiatively help the universities, etc. 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 the 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 enhance common security measures implemented through the entire organization as well as technological measures for protecting the technological information from advanced cyberattacks and effective measures against supply chain risks.

[43] Revised by the Ministry of Internal Affairs and Communications in December 2020. These Guidelines explain the thinking behind information security policies and their content to serve as a reference for local governments when formulating and revising information security policies.

[44] Approved by the Cabinet on December 25, 2020. This presents the government's policy based on the discussions held in the working group on digital transformation-related bills under the digital government cabinet meeting, concerning the future of digital society, thinking behind the revision of the Basic Act on IT, and thinking behind the establishment of the Digital Agency (tentative name).

4.2.6 Seamless information sharing and collaboration by multiple stakeholders and application of knowledge gained 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 the whole of 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 improve a national CERT/CSIRT framework. By doing so, the national government will advance efforts to raise the nation’s overall level of cybersecurity 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 CEPTOAR and ISAC[45], 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 the whole of nation against cyberattacks, the national government will strengthen collaboration between information sharing systems, including the Cybersecurity Council, Cybersecurity Response and Coordination Center, and specialized agencies that have sufficient technical capabilities and expertise in communication and coordination with stakeholders in and outside Japan, as part of efforts to improve 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 at all times, from during large-scale international events such as the EXPO 2025 to ordinary times.

4.2.7 Enhancement of readiness to respond to massive cyberattacks, etc.

Given that cyberspace and real space are becoming increasingly intertwined and the impact of incidents may spread over a wide area, and based on damage forecasts that take these into

[45] ISAC is an abbreviation for Information Sharing and Analysis Center. ISAC collects information on cybersecurity and analyzes it. The analyzed information is shared among ISAC members and used for security measures.

consideration, the national government will strengthen seamless and whole of nation 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 stakeholder 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 by a military unit with advanced cyber capabilities targeting the critical infrastructure of another country. As greater segments of society become increasingly digitalized, cyberattacks have the risk of rapidly developing into a graver situation. Influence operations carried out using cyberspace and cyberattacks, which are difficult to attribute and whose incurred damages are hard to assess, 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 in which state involvement is suspected 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.[46] In addition, it is observed that China, Russia, and North Korea are continuing to build the cyber capabilities of their military and other institutions.[47] 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 commands and strengthen the ability to respond to cyberattacks.[48]

Under these circumstances, 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’”), Japan-US Foreign Ministers’ meeting and Japan-US Defense Ministerial Meeting held in March 2021, the ministers confirmed the importance of further strengthening this field. In addition, as national security has been expanding its scope to include economic and technological fields in recent years, Japan is likewise collaborating with its ally and like-minded countries to address conflicts over technological

[46] Refer to the G7 Summit Communique (June 2021), G7 Foreign and Development Ministers’ Meeting Communique (May 2021), Final Report of the Panel of Experts Assisting the UN Security Council Sanctions Committee on North Korea (March 2021), National Cyber Strategy of the United States of America (September 2018), and Cyber Strategy, US Department of Defense (September 2018) for more information about cyberattacks carried out by China, Russia, and North Korea.
In addition, the Overview of Threats in Cyberspace 2021 issued by the Public Security Intelligence Agency and Review and Prospects of Public Order issued by the Security Bureau of the National Police Agency (December 2020) refer to announcements made by the United States and others on individual cases, in which the involvement of Chinese, Russian, and North Korean military and intelligence agencies is pointed out. See footnote 55 as well for more information on China.

[47] Defense of Japan 2021, Ministry of Defense (Cabinet report of July 13, 2021)

[48] Defense of Japan 2021, Ministry of Defense (Cabinet report of July 13, 2021)

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, Japan will place a higher priority on cyber issues in diplomatic and national security agenda. At the same time, Japan 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, Japan will promote its basic principles in the international arena. Japan will continue to play active roles to advance the rule of law in cyberspace and establish international rules in line with Japan's basic principles, in collaboration with its ally and like-minded countries.

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

The promotion of the rule of law in cyberspace is important for the peace and stability of the international community and Japan's national security.

To ensure "a free, fair and secure cyberspace" on a global scale, Japan will promote 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 were 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. In the UN and elsewhere, Japan will actively promote its views on the application of international law, and collaborate with its ally and like-minded countries to ensure "a free, fair and secure cyberspace" by actively engaging in the practice of norms in cyberspace, based on its stance that the existing international law applies in cyberspace as well. Through such activities, Japan will work to participate in discussions 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 enhance the deterrent capability of the Japan-US Alliance as a whole.

As for measures against cybercrimes, Japan will use existing international frameworks such as the Convention on Cybercrime and advance its universalization and enhancement. At the same time, Japan 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.[49] 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

[49] The Prague Proposals refer to the Chairman Statement announced at the Prague 5G Security Conference in May 2019.

approach to internet governance such as the Internet Governance Forum are developing as well.[50]

Meanwhile, in light of the fact that proposals that may be incompatible with the existing order are being put forward, Japan will continue to deliver its basic principles to the international community, and actively contribute to the formulation of new international rules in line with them. In addition, Japan 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. Japan will work with its 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 Japan's capabilities for defense, deterrence, and situational awareness

Amidst an increasingly severe security environment surrounding Japan, cyberattacks have been taking place against governmental bodies, critical infrastructure operators, companies and academic and research institutions possessing advanced technologies. There are cases that could threaten to undermine the foundations of democracy. Furthermore, some of these attacks are suspected of state involvement.

Given the situation, in order to protect Japan's national security interest from cyberattacks, it is vital to secure Japan's resilience against cyberattacks and increase Japan's ability 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.

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 the National center of Incident readiness and Strategy for Cybersecurity 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 from normal times and proceed with the initiatives. When necessary, deliberation and decision will be made at the National Security Council.

As part of the government's overall effort concerning national security, the Ministry of Defense and the SDF will undertake various initiatives based on the National Defense Program Guidelines for FY2019 and beyond, and fundamentally strengthen cyber defense.

(1) Increasing defense capabilities

(i) Mission Assurance

It is the mission of government agencies to protect and support the people's lives and socio-economic activities. A suspension of their functions would be a significant concern for national security. The execution of their mission relies on the services provided by business operators which maintain critical infrastructure and other systems. These operators also have important missions to provide the services indispensable for the people and society.

[50] 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."

From the perspective of mission assurance, government agencies and critical infrastructure operators, etc. must continue to advance efforts to ensure cybersecurity. The government will advance further protection including risk reduction for networks where critical information concerning national security is handled. In addition, the government will steadily conduct joint exercises by the SDF and US military to defend critical infrastructure and services that underpin their activities. The Ministry of Defense and the SDF will strive to fundamentally strengthen cyber defense capabilities, for example, by enhancing the posture of cyber-related units.

(ii) Protection of Japan's Advanced Technologies and Defense Related Technologies

As information crucial to Japan's national security is being targeted, further measures including risk reduction are needed to protect technologies relevant to its national security, such as technology related to space, nuclear power, and other advanced technology. As for the defense industry in particular, Japan 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.

(iii) Measures Against the Malicious Use of Cyberspace by Terrorist Organizations

Cyberspace offers a place where individuals and organizations can exchange information and express their thoughts freely. It serves as one of the foundations of democracy. On the other hand, it is necessary to prevent the malicious use of cyberspace by terrorist organizations, such as spreading and demonstrating violent extremism, recruiting of people into the organizations, and gathering funds for organizations. For that reason, Japan will continue to work together with the international community and implement necessary measures against the activities of terrorist groups exploiting cyberspace, while also guaranteeing the basic human rights including the freedom of expression.

(2) Enhancing deterrence capabilities

(i) Measures for Effective Deterrence

Existing international law, including the United Nations Charter, in its entirety is applicable in cyberspace.[51] Internationally wrongful acts committed by a state in cyberspace entail state responsibilities and a state that is the victim of such acts may, in certain circumstances, resort to proportionate countermeasures and other lawful measures against the state responsible for the wrongful acts. Under some circumstances, cyberattacks could amount to the use of force or an armed attack under international law.[52]

Based on this recognition, in order to deter malicious cyber activities and protect the people's safety and rights, Japan will continue to have close coordination with its ally and like-minded countries from normal times, and will take resolute responses against cyber threats, including those possibly sponsored by states, utilizing political, economic, technological, legal, diplomatic, and all other viable and effective

[51] In the 2015 report of the fourth session of the United Nations Group of Governmental Experts, it was confirmed that existing international law, including the entire UN Charter, will be applied in cyberspace, and this was reconfirmed in the 2021 report by the UN Open-Ended Working Group.

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

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 fulfilling the requirement of implementing the Article V of the Japan-U.S. Security Treaty. In addition to employing capability to disrupt the opponent's use of cyberspace for an attack against Japan, Japan will take due steps including the use of diplomatic means (e.g., condemning cyberattacks) and criminal prosecution. As an example of diplomatic means[53], in July 2021, Japan issued a Foreign Press Secretary's comment[54] firmly condemning cyberattacks conducted by a cyberattack group which the Chinese government is highly likely behind, and cyberattacks[55] to have involved a cyberattack group which the Chinese People's Liberation Army (PLA) was highly likely behind,[53] and indicating its will to take strict measures against these activities. Examples of criminal prosecution include investigations of a case in which the police sent an investigation report to prosecutors in April 2021. These investigations led to the conclusion that the PLA was highly likely to be involved in the cyberattacks by a group with close links to the PLA against entities including Japanese companies. Operational units established within the police organization will continue to crack down on such activities.

Since cyberattacks have the risk of rapidly developing into a graver situation, Japan will quickly respond to incidents by seamlessly transitioning throughout the process of escalation from peacetime to large-scale cyberattacks and then to armed attacks. In addition, Japan will continue to maintain and strengthen the deterrence of the Japan-US Alliance, in light of the outcome of the Japan-US "2+2" in March 2021.

(ii) Confidence Building Measures

Japan will work to build confidence among states in order to prevent the occurrence of unforeseen circumstances and deterioration of the situation caused by cyberattacks. The highly anonymous and covert nature of cyberspace has the risk of inadvertently heightening tensions among states and aggravating the situation. In order to prevent such accidental or unnecessary confrontations, it is important to build up international communication channels as a confidence building measure during normal times in preparation for the occurrence of incidents that extend beyond national borders.

It is also necessary to increase transparency and build confidence between states through the proactive information exchange and policy dialogues in bilateral and multilateral consultations. Japan will also cooperate with other states to utilize a mechanism for coordinating issues regarding cyberspace.

[53] To date, Japan has also 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 its ally and like-minded countries.

[54] A Foreign Press Secretary's comment was issued firmly condemning cyberattacks conducted by a group known as "APT40," which the Chinese government is highly likely behind (July 19, 2021).

[55] A case in which the Metropolitan Police Department sent an investigation report to the Tokyo District Public Prosecutors Office in April 2021, naming a Chinese Communist Party member as a suspect. With regard to this case, the following comment was made in the press conference by the Chief Cabinet Secretary on April 20, 2021:"We are aware that the investigation revealed that the contracted Japanese rental server was used to launch cyberattacks against JAXA (Japan Aerospace Exploration Agency) and other organizations, and that it is highly likely that an Advanced Persistent Threat group called Tick, which the Unit 61419 of the Chinese People's Liberation Army is behind, was involved in the attacks."

(3) Strengthening cyber situational awareness capabilities

(i) Increasing the Capabilities of Relevant Governmental Bodies

Situational awareness capabilities are the foundation of defense and deterrence capabilities. In order to deter increasingly serious cyberattacks and influence operations using cyberspace, in addition to enhancing response capabilities, adequate capabilities to detect, investigate, and analyze cyberattacks are necessary to identify the attackers and hold them accountable. To this end, Japan will continue to improve such abilities of relevant agencies both in terms of quality and quantity, and advance efforts to further clarify the actual situation of cyberattacks, leveraging the nationwide networks, technical teams, and human intelligence of relevant agencies.

In addition, the government will proceed with wide ranging considerations of any effective means including the development and securing of cybersecurity human resources with high-level analytical capabilities, and development and utilization of technologies for detecting, investigating, and analyzing cyberattacks. The government will also carry out initiatives related to counter-cyber intelligence.[56]

(ii) Threat Information Collaboration

Information sharing among relevant ministries and agencies within the government and with its ally and like-minded countries will be advanced with the aim of accurately responding to and deterring diverse threats of cyberattacks, including those suspected of state involvement and those conducted by non-governmental organizations. The government will also strengthen the threat information sharing and collaboration framework within the government led by the Cabinet Secretariat.

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. To this end, Japan will advance the sharing of expertise and policy coordination, as well as international collaboration and capacity building support related to cyber incidents.

(1) Sharing expertise and policy coordination

As conflicts over international rules and technological foundation come to the fore, Japan will strengthen collaboration with its ally and like-minded countries. This will include high-level cross-ministerial bilateral talks including cyber dialogues with the US and like-minded countries, etc. and multilateral talks, 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. Japan will actively advance cooperation with the US, Australia, and India, as well as ASEAN,[57] and other countries in the field of cybersecurity toward the realization of “Free and Open Indo-Pacific (FOIP).”

Japan 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 international

[56] Intelligence defense activity against intelligence activity by foreign countries using information and communication technology

[57] Association of Southeast Asian Nations

conferences. In addition, Japan will enhance the communication of information about Japan’s cybersecurity policies to international audiences, and Japan will make international contributions by sharing its experience at the Tokyo Games among others with other countries.

(2) Strengthening international collaboration for incident response

To respond rapidly to cyber incidents and prevent the spread of damage, Japan will continue to enhance the sharing of information related to cyberattacks (e.g., information about vulnerabilities and IoC[58]) with international partners from normal times, and consider disseminating information jointly with other countries. Japan will enhance its international presence in the cyber community. To this end, Japan will not only promote collaboration among CERTs and participate in international cyber exercises, but Japan will also lead such exercises and build trust for collaborative response, as well as serving as an information hub.

(3) Supporting for capacity building

Today, as interdependence across borders has deepened, it is not possible for Japan to secure peace and stability only by itself. Global coordination to reduce cybersecurity vulnerabilities and to aim for their elimination is essential in contributing to ensuring Japan’s national security. From this standpoint, assisting capacity building in other states directly leads to the security of the entire cyberspace and contributes to the improvement of the global security environment including Japan, as well as ensures the stability of the lives of Japanese residents and the activities of Japanese companies that depend on critical infrastructure in recipient countries and promotes the development of the sound use of cyberspace there.

Other countries are providing various capacity building supports for developing countries. Under Japan’s basic principles, and based on the basic policy on capacity building support that sets forth enhancing efforts including industry-academia-government collaboration, diplomacy, and national security, Japan 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 organizations such as the World Bank, industry and academia.

By ensuring cybersecurity in this manner, Japan will promote the achievement of the SDGs and help maintain cyber hygiene. Moreover, Japan will also support capacity building not only through human resource development and cyber exercises, but also in understanding and practicing international legal principles, policy formation, establishment of technical standards, and fields that form the next-generation cyber environment such as 5G and IoT. Additionally, Japan will boost overseas business expansion in cybersecurity.[59]

In addition to these efforts, Japan will fundamentally 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 in capacity building, and in consideration of the region’s geopolitical significance.

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

[59] Infrastructure System Overseas Expansion Strategy 2025 (decided by the Infrastructure Strategy Economic Cooperation Meeting on June 17, 2021)

4.4.

Cross-Cutting Approaches to Cybersecurity

In order to achieve the three policy goals—"Enhancing socio-economic vitality and sustainable development," "Realizing a digital society where the people can live with a sense of safety and security," and "Contributing to the peace and stability of the international community and Japan's national security"—it is important to work on research and development, human resource development, and awareness raising as a foundation for the policy goals from both a cross-cutting and medium- and long-term perspective.

The government will advance initiatives keeping in mind the three directions of "Advancing digital transformation and cybersecurity simultaneously," "Enhancing the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated," and "Enhancing initiatives from the perspective of Japan's national security."

4.4.1 Advancement of R&D

Cybersecurity research is extremely important in this field to pursue R&D with a practical approach, considering threat information and user needs. On the other hand, international competitiveness in R&D and an industry-academia-government ecosystem must be established in Japan as a foundation for the effective implementation of practical R&D. The government will pursue initiatives aimed at building such a foundation from a medium- to long-term perspective, as well as practical initiatives based on such efforts.

As it is also important to consider the progress of digital technologies, the government will advance R&D taking medium- to long-term technological trends into account.

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

The field of cybersecurity research is new and growing, with researchers flowing in from various fields and 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. Together with the field of digital technology, this has become an important field of research as the use of digital technology becomes an integral part of cybersecurity measures.

While the number of cybersecurity researchers has been increasing in Japan as well, societal 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 its own cybersecurity measures and technology, the government 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.

Specifically, the government will promote the use of measures provided by relevant ministries to promote research and government-industry-academia collaboration that will become sources of scientific understanding and innovation, while enhancing such collaboration and focused research coupled with voluntary development efforts by the research community. In addition, the government will strive to create an environment where researchers can engage in research with peace of mind by providing fully equipped research environments.

To establish a government-industry-academia ecosystem, voluntary development efforts by each stakeholder is essential. The government will follow up on the status of these efforts as the government advances its initiatives.

(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, possible occurrence of new threats due to the progress of AI, IoT, etc.), as well as a perspective of national security, the government will advance practical R&D related to cybersecurity in Japan along the following directions.

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

The government will advance R&D and practical application of verification technologies to verify that malicious programs and circuits are not built into software and hardware. Specifically, the government will advance the establishment of a comprehensive verification platform through the demonstration of high-level verification services to test the trustworthiness of IoT devices, development of a system to ensure the security of 5G components comprehensively and continuously, and R&D and practical application of technologies to detect malicious functions through the analysis of chip design circuits and observation of system and service behavior, and of verification technologies toward the realization of a secure Society 5.0.

In light of these initiatives, the government will work as one to develop an implementation framework for conducting technical verification of ICT device and service security, with the aim of ensuring the trustworthiness of the entire supply chain, considering efforts to secure and foster domestic technologies and possible uses in government procurement.

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

With the aim of cultivating and developing the cybersecurity industry, the government will improve the effectiveness verification platform so that products and services can be used with peace of mind, and improve the business environment of domestic industries such as by creating businesses that meet the needs of SMEs. The government will also match businesses concerning seeds and needs and promote their market expansion.

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

The government will strengthen information sharing platforms and the technology to observe, identify, and analyze cyberattacks while using AI and other advanced technologies, in order to appropriately respond to the development of cyberattack threats, such as increasingly sophisticated, complex, and diversified cyberattacks and increased vulnerabilities due to the spread of IoT devices.

Specifically, in order to respond to sophisticated and complex cyberattacks and unknown threats to IoT as it becomes increasingly widespread going forward, the government will develop more advanced cyberattack observation technology using honeypot and other technologies that flexibly respond to wide-area darknets and different attack types, and perform R&D on AI-based technology to automate the analysis of attack behavior. Moreover, to identify and analyze the attack behavior of Advanced Persistent Threats and respond rapidly, the government will develop a more sophisticated platform for luring cyberattacks and expand its usage, collecting specific behavior samples and performing R&D on technology to rapidly detect and analyze unknown Advanced Persistent Threats and other attacks. In addition, the government will perform R&D on efficient wide-area network scans that will realize improved traffic volume control and accuracy to identify vulnerable IoT devices with high reliability and take security countermeasures. The government will also advance initiatives to build and share an intellectual foundation for collecting, accumulating, analyzing, and providing cybersecurity information within the country.

(iv) Advance research of cryptography, etc.

It is expected that existing encryption technologies will become compromised when practical, large-scale quantum computing is realized. With this in mind, the government will establish a foundation for advancing cutting-edge research on post-quantum cryptography and quantum cryptography to ensure security. The government will also establish lightweight encryption technology to enable secure telecommunications even with devices with limited resources such as IoT devices.

Specifically, in light of the realization of practical and large-scale quantum computing, spread of IoT, and developments in new encryption technology, the government will engage in ongoing discussions on ensuring the security and trustworthiness of encryption technology and promoting its widespread adoption, and deliberate the creation of a guideline on post-quantum cryptography and lightweight cryptography. The government will also advance R&D to establish quantum information and telecommunications technology that uses quantum cryptography, which is extremely difficult to eavesdrop on and tamper with, and technology for using quantum key distribution in micro-satellites.

The government will advance these efforts of relevant ministries during the planning period of the strategy, follow up on the status of efforts including efforts of relevant ministries concerning the promotion of research and government-industry-academia collaboration, and conduct inspections and any necessary re-arrangement by mapping efforts and so on. In addition to advancing the widespread adoption and practical application of the results of R&D, the government will also promote information exchange by relevant ministries toward the use of new Japan-made technology by government agencies as part of this effort.

(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"[60] and other advanced network technologies. In particular, it will be necessary to take the progress of AI, quantum, and other advanced technology into consideration, and the government will advance efforts based on the following understanding of the situation.

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

AI technology has been advancing at an accelerated pace in recent years, and by being applied around the world, it is causing a major impact on a wide range of industries and social infrastructure. Its relationship with cybersecurity can be understood from three perspectives: cybersecurity measures using AI, cyberattacks using AI, and security for protecting AI itself.

As for cybersecurity measures using AI (AI for Security), security products and services using AI are actually being commercialized. The government will continue to support AI-based cyber measures pursued by the private sector based on a comprehensive strategy on AI technology, while moving forward to establish highly efficient and elaborate countermeasure technology that uses AI in the prevention,

[60] 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.

detection, and response phases.

From the perspective of addressing cyberattacks that utilize AI, "AI for Security" initiatives will also be important in terms of preventing the asymmetric relationship between the attackers and the defense side from expanding further. To this end, it is important to take a proactive approach to research by gaining insights from the viewpoint of the attacker and enhance security measures pre-emptively.

As for security to protect AI itself (Security for AI), the vulnerabilities[61] in AI are still not fully understood. Academically, for example, studies that attempt to generate hostile samples that may induce false recognition of machine learning and studies on how to defend against such false recognition are increasing overseas. In Japan, the government will promote basic research and continue to study technical issues in a long-term effort aimed at realization five to ten years down the road.

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

The advancement of quantum computers has given rise to the possibility that the public key encryption technology underpinning today's internet security may be deciphered. For this reason, post-quantum cryptography has become an increasing focus of study around the world. Japan has likewise announced its plans to establish a foundation for advancing cutting-edge research on post-quantum cryptography, etc. to ensure security.

Meanwhile, post-quantum cryptography also carries the risk of being compromised, so countries around the world are rapidly advancing R&D on quantum communications and cryptography, which is guaranteed to be secure in principle, with the understanding that this is a major threat concerning national security. Japan will likewise pursue R&D on quantum communications and cryptography, as well as their commercialization and standardization, as an alternative equipped with confidentiality, integrity, and superior international competitiveness with an eye to marketization, and as a secure means of storing critical information. This will be done from the perspectives of ensuring the safety and security of the state and its people, and strengthening industrial competitiveness.

In addition to the above, Japan will constantly study technical issues that it must actively address, considering various technical trends, including Beyond 5G, from a medium- to long-term perspective.

4.4.2 Recruitment, development, and active use of human resources

With cyberattacks becoming increasingly complex and sophisticated, it is imperative for companies to develop and secure human resources needed to ensure cybersecurity in order to ensure business continuity and create new value. While a lack of cybersecurity human resources has long been pointed out in Japan, progress has also been made in public-private initiatives to train operators and experts, including promotion of certification programs, tests, exercises, and relearning. Given an understanding of the current situation and the spread of efforts toward digitalization, the government need to further continue and deepen efforts by the public and private sectors both in terms of quality and quantity.

Moreover, in order for digitalization to be advanced along with measures to address accompanying threats, it is important to create an environment where cybersecurity human resources, regardless of gender, can play active

[61] For example, possible threats include data poisoning attacks (attacks that involve polluting training data to cause decision errors).

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, the government 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) Creating an environment for human resources needed for “DX with Cybersecurity”

In order for digitalization to be advanced throughout society along with efforts to ensure cybersecurity (DX with Cybersecurity), it is important to link supply and demand—both demand for talent and work in security and other fields that accompanies digitalization within companies and organizations, and supply of talent and work through the inflow of young workers and other human resources provided in response to societal demand or through appropriate matching, must be increased in a way that creates a virtuous cycle.

An environment must be created where security human resources can play an active role, from the perspectives of establishing functions within companies and organizations, as well as mobility and matching of human resources, not to mention securing the quality and quantity of human resources development programs for operators and engineers. Otherwise, efforts to advance digitalization of the economy and society will fall into a vicious cycle and be faced with uncertainty.

For this to happen, management and everyone in a company or an organization who is engaged in digital transformation or is advancing it 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. It will be important to raise executive awareness while creating an environment where the necessary skills and basic knowledge can be acquired.

(i) Creating an environment where people can gain 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 involved in advancing digital transformation in companies and organizations, 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 the government will enhance “strategy management level personnel” through these efforts.

However, human resources development programs such as training and seminars related to IT literacy and Plus Security knowledge are not necessarily prevalent in society. For this reason, as part of preparing the environment, the government will address both the demand and supply sides of human resources development programs with the aim of forming and developing markets.

In various companies and organizations working on “DX with cybersecurity,” there is an increasing need for human resources (including executives) who do not necessarily have relevant expertise or work experience to gain IT literacy and Plus Security knowledge so that they may engage in digitalization going forward. This means that there is potentially large demand. Accordingly, it is important to encourage employees in these companies and organizations to participate in human resources development programs, and to provide staff training opportunities. The government and relevant agencies and organizations will lead awareness-raising activities to urge companies, etc. to engage in efforts that will lead to the manifestation of such demand.

In addition, the government and relevant agencies, companies, and educational institutions that provide human resources development programs will provide leading and fundamental programs, and actively communicate information about public and private sector efforts through, for example, a portal site that lists compatible programs. These initiatives will be undertaken with the aim of creating a system where companies and organizations can expect a certain level of quality from the supply side. The use of tools that will provide a deeper understanding of laws and regulations will be promoted to facilitate collaboration with experts aimed at advancing measures.

(ii) Establishing functions within companies and organizations, efforts related to the mobility and matching of talent

Amid a rise in the digitalization of work, network connection of products, development of digital services, and coordination between digital services, future practices will need to focus on rapid and flexible development and response, as well as monitoring and response that address new risks. In particular, the concept of “security by design” will become ever more important in the practice of the former, with collaboration between planning, development, and operation departments and the security functions of companies and organizations taking on greater importance. On the other hand, it is also true that there are not enough examples that can be referenced nor sufficient accumulation of human resources to aid the establishment and promotion of these functions.

In terms of providing a place for human resources to play an active role, the government will likely see more opportunities to use flexible modes of employment, such as secondary and concurrent employment, in light of the changes in the employment environment and clarification of how work hours should be managed, which resulted from the effort to respond to the COVID-19 pandemic. Given moves toward digital transformation, demand for human resources will likely increase among government agencies and local governments to handle digital-related work, including operational reform in the administrative field. To advance “DX with Cybersecurity” as a society-wide effort, the government needs 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.

Therefore, the government will consider these trends and the even distribution of human resources as the government promote practices related to building functions and securing and developing IT and security personnel inside companies and organizations. To this end, the government will ascertain the situation concerning human resource needs, conduct awareness-raising activities in light of actual incidents, promote the use of reference guides, collect and compile leading examples of function building and people playing an active role in companies and organizations, actively communicate information through portal sites, and provide relearning opportunities.

As local regions and SMEs are faced with a particularly dire lack of security talent, the government will provide know-how and networks that will be useful in applying practices through mutual help initiatives in communities, and by building an ecosystem and promoting collaboration between industry and educational institutions.

(2) Addressing increasingly sophisticated and complex threats

The government 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.

For the training of operators and experts, public-private initiatives are being advanced, such as developing and improving certification systems, implementing programs for young talent and programs targeting operators engaged with industrial control systems, providing exercise environments, and promoting relearning. At the same time, the government will address recent threat trends, incorporate diverse perspectives and excellent ideas regardless of gender or educational background, further enhance efforts toward the development of human resources equipped with practical response capabilities, and develop and improve content.

The government will also build a common foundation for developing human resources to handle cybersecurity as a society-wide effort, and make it available to industry and academia so that educational institutions and educational businesses can provide exercise services, while maintaining the quality of instructors.

To facilitate the career development and matching of these human resources, the government will provide information about various people playing an active role as leading examples, 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 the SDF.

(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 ministries, local governments, private sectors, and incorporated administrative agencies.[62] Based on this thinking, all government agencies will work together to enhance initiatives, based on a policy aimed at reinforcing the system of using advanced outside experts, promoting recruitment of successful candidates from the newly established “digital division” of the Recruitment Examination for National Public Employees, and enhancing training in light of the progress of digitalization.

Based on this policy, each ministry will develop a human resources recruitment and development plan, 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, etc. In addition, the government will follow up on the plan each fiscal year and further enhance initiatives.

In particular, to address advanced cybercrimes and national security, the government will not only enlist the help of advanced outside experts but also develop and recruit our own advanced experts within government agencies.

[62] This is also indicated in the “Basic Policy on Reform toward the Realization of a Digital Society” (approved by the Cabinet on December 25, 2020).

4.4.3 Collaboration based on full participation and awareness raising

As cyberspace and physical 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 undertake basic efforts even during normal times as public hygiene activities in cyberspace, and to be able to address various risks, as with crime prevention and traffic safety measures in physical space. It will be important for the public and private sectors to work together on raising awareness and providing information to reinforce behavior that allows the people to acquire literacy and 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. The government is required to build a system that enables stakeholders to collaborate and cooperate according to their mutual division of responsibilities while respecting the autonomous activities of various communities such as regions, companies, and schools, and to play a role in supporting such a system.

With this understanding, the government have formulated a detailed action plan toward "collaboration based on full participation" so that stakeholders in industry and academia and the public and private sectors can engage in smooth and effective awareness-raising activities, and the government have advanced initiatives with a focus on local regions, SMEs, and young people. The idea of "Cybersecurity for All" that this strategy sets forth includes the thinking that all stakeholders must be independently aware of their own role and engage in cybersecurity. As digital transformation progresses, it is expected that a wider range of people will participate in cyberspace. Under these circumstances, it will be necessary to steadily advance the action plan, follow up on the status of efforts, and make ongoing improvements. Moreover, the government will consider reviewing the action plan including the response to the elderly.

In addition, guidelines and various explanatory documents are being prepared, particularly in response to the recent changes in people's behavior and corporate activities, such as more and more people engaging in remote work and using cloud services. Including these, the government will take necessary steps with respect to the nature (content) of information provision and awareness-raising activities.

5 Implementation Framework

This strategy calls for ensuring cybersecurity in line with the digital transformation that the government is pursuing.[63] The government has been promoting a policy of improving cybersecurity measures to ensure Japan's national security.[64]

A concerted effort by the whole of government is needed to promote and implement cybersecurity policy in order to ensure a free, fair and secure cyberspace in line with Japan's cybersecurity policies. The Cybersecurity Strategic Headquarters (hereinafter referred to as the "Headquarters") will make further efforts 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, the National center of Incident readiness and Strategy for Cybersecurity (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 Headquarters.

The Headquarters will work closely with the newly established Digital Agency on formulating basic development policies.[65] Crisis management needs to be further enhanced as well. The Headquarters will collaborate and share information with the crisis management organs, including headquarters for emergency response to terrorism, when established. Furthermore, the Headquarters will respond to issues concerning national security in close coordination with the National Security Council. In such cases, the relevant ministries and agencies will work together under the overall coordination by the National Security Secretariat.

The Headquarters will work together with relevant ministries and agencies to actively communicate this strategy to stakeholders both in Japan and abroad, in order to encourage each stakeholder to take practical actions in response to changing cybersecurity risks, and further understanding by foreign governments of Japan's stance and enhance deterrence against attackers with the importance of international cooperation in mind.

Based on the direction indicated in this strategy, the 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, the government 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. To enable comprehensive response by the whole of government against cyberattacks, the Headquarters will improve a

[63] "Priority Plan toward the Realization of a Digital Society" (approved by the Cabinet on June 18, 2021)

[64] The National Security Strategy (Cabinet decision on December 17, 2013) states that "cyberspace is necessary for promoting both economic growth and innovation through the free flow of information in cyberspace. Protecting cyberspace from the above-mentioned risks is vital to secure national security."

[65] Pursuant to Article 43 of the Supplemental Provisions of the Act for Establishment of the Digital Agency (Act No. 36 of 2021), the minister in charge of digital affairs has been added as a member of the Cybersecurity Strategic Headquarters.

national CERTs/CSIRTs framework.

Going forward, the 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.

Responsibility Assignment Matrix for Policy Approaches

Appendix

Contents	Organizations* (◎：Responsible, ○：Involved)
4.1. Enhancing socio-economic vitality and sustainable development —Advancing DX with Cybersecurity	
4.1.1 Raising executive awareness	◎：NISC[66], MIC, METI ○：FSA
4.1.2 Promotion of “DX with Cybersecurity” among local regions and SMEs	◎：NISC, MIC, METI
4.1.3 Building a foundation for ensuring trustworthiness of supply chains that support new value creation	
(1) Ensuring trustworthiness of supply chains	◎：MIC, METI ○：Other Ministries and Agencies
(2) Ensuring trustworthiness of data flow	◎：DA, MIC, METI ○：MOJ
(3) Ensuring trustworthiness of security products and services	◎：METI ○：NISC, MIC
(4) Practical application of advanced technology and innovation	◎：NISC, CAO, MIC, METI ※CAO：Director General for Science and Technology Policy
4.1.4 Advancing digital/security literacy with no one left behind	◎：NISC, MIC, MEXT ○：DA, METI
4.2. Realizing a digital society where the people can live with a sense of safety and security	
4.2.1 Providing a cybersecurity environment which protects the people and society	◎：CAS, NPA*1, MIC, METI ○：MOFA, MOF, MOD, Other Ministries and Agencies ※CAS：NSS
(1) Building a safe and secure cyber environment for users	◎：NISC, CAS, CAO, FSA, CCA, Digital Agency, MIC, MHLW, METI, MLIT ○：CAS, CAO, Imperial Household Agency, NPA*1, MOJ, MOFA, MEXT, MAFF, MOE, MOD ※CAS（◎）：Drone Policy Office ※CAO（◎）：Director General for Science and Technology Policy ※CAS（○）：CCS, Cabinet Affairs Office, CIRO, Growth Strategy Council Bureau ※CAO（○）：Office for Promotion of Regional Revitalization

[66] NISC is the abbreviation for National center of Incident readiness and Strategy for Cybersecurity. NISC (formerly called National Information Security Center) was established in the Cabinet Secretariat on January 9, 2015, as an organization which handles the administrative work of the Cybersecurity Strategic Headquarters. NISC is responsible for the function of the cybersecurity control tower in Japan. Assistant Chief Cabinet Secretary (in charge of Situations Response and Crisis Management) concurrently holds the post of Director-General of NISC.

(2) Strengthening cooperation with new providers in cyberspace	◎：NISC, DA, MIC, METI
(3) Addressing cyber crimes	◎：CAO, NPA[*1], MIC, MOJ, METI ※CAO：SPPC
(4) Deploying comprehensive cyber defense	◎：NISC, CAS, NPA[*1], MIC, MOFA, METI, MOD ※CAS：NSS, CIRO
(5) Ensuring trustworthiness of cyberspace	◎：NISC, CAS, CAO, FSA, MIC, MEXT, MHLW, METI, MLIT ※CAS：NSS ※CAO：SPPC
4.2.2 Ensuring cybersecurity integral with digital transformation (led by the Digital Agency)	◎：NISC, CAO, DA, MIC, MHLW, METI ※CAO：Office for Social Security and Tax Number System
4.2.3 Promotion of efforts by stakeholders which underpin the socio-economic infrastructure (1) (Government agencies, etc.)	◎：NISC, DA, MIC, MHLW, METI ○：NPA[*2], CAO, CCA, MOFA, MOF, MEXT, MAFF, MLIT, MOE, MOD
4.2.4 Promotion of efforts by stakeholders which underpin the socio-economic infrastructure (2) (Critical infrastructure)	
(1) Advancing protection of critical infrastructure based on public-private collaboration	◎：NISC, FSA, MIC, MHLW, METI, MLIT ○：NPA[*1]
(2) Support for local governments	◎：NISC, CAO, MIC ○：DA, MHLW ※CAO：SPPC, Office for Social Security and Tax Number System
4.2.5 Promotion of efforts by stakeholders which underpin the socio-economic infrastructure (3) (Universities, education and research institutions, etc.)	◎：MEXT ○：NISC
4.2.6 Seamless information sharing and collaboration by multiple stakeholders and application of knowledge gained through efforts toward the Tokyo Games, etc.	◎：NISC,CAS,NPA[*1],MOJ ※CAS：Secretariat of the Headquarters for the Tokyo 2020 Games
(1) Advancing information sharing and collaboration according to each field and issue	◎：NISC, FSA, MIC, MHLW, METI, MLIT
(2) Establishing an information sharing and collaboration system that contributes to comprehensive cyber defense	◎：NISC, CAS, NPA[*1], MIC, MOFA, METI, MOD ※CAS：NSS, CIRO
4.2.7 Enhancement of readiness to respond to massive cyberattacks, etc.	◎：NISC, CAS, CAO, NPA[*1], FSA, METI ※CAS：CCS ※CAO：SPPC
4.3. Contributing to the Peace and Stability of the International Community and Japan’s National Security	
4.3.1 ｢Ensuring “a free, fair and secure cyberspace”	
(1) Promoting the rule of law in cyberspace (formulating rules that contribute to Japan’s national security)	◎：NISC, NPA[*1], MOJ, MOFA ○：MIC, METI, MOD
(2) Formulating rules in cyberspace	◎：NISC, MOFA, METI ○：NPA[*1], MIC, MOD

4.3.2 Strengthening Japan's capabilities for defense, deterrence, and situational awareness	◎：CAS, MOD ○：NPA[*1], MOFA, MOF, METI ※CAS：NSS
(1) Increasing defense capabilities	◎：NISC, CAS, NPA[*1], MOJ, MOFA, MEXT, MOD ○：CAO, MIC, MHLW, MAFF, METI, MLIT, MOE ※CAS：CIRO
(2) Enhancing deterrence capabilities	◎：NISC, CAS, NPA[*1], MOFA, METI, MOD ○：MIC, MOF, Other Ministries and Agencies ※CAS：NSS
(3) Strengthening cyber situational awareness capabilities	◎：CAS, NPA[*1], MOJ, METI, MOD ○：MIC, MOFA ※CAS：CIRO
4.3.3 International cooperation and collaboration	
(1) Sharing expertise and policy coordination	◎：NISC, NPA[*1], MIC, MOJ, MOFA, METI, MOD ○：Other Ministries and Agencies
(2) Strengthening international collaboration for incident response	◎：NISC, METI, MOD ○：NPA[*1], MOFA
(3) Supporting for capacity building	◎：NISC, NPA[*1], MIC, MOFA, METI, MOD ○：MOJ
4.4. Cross-Cutting Approaches to Cybersecurity	
4.4.1 Advancement of R&D	
(1) Strengthening international competitiveness in R&D and building an industry-academia-government ecosystem	◎：NISC, CAO, MIC, MEXT, METI ※CAO：Director General for Science and Technology Policy
(2) Advancing practical R&D	◎：NISC, CAO, MIC, MEXT, METI ○：Other Ministries and Agencies ※CAO：Director General for Science and Technology Policy
(3) Taking medium- to long-term technological trends into consideration	◎：NISC, CAO, MIC, MEXT, METI ※CAO：Director General for Science and Technology Policy
4.4.2 Recruitment, development, and active use of human resources	◎：NPA[*1], MEXT, MHLW
(1) Creating an environment for human resources needed for "DX with Cybersecurity"	◎：NISC, MIC, METI ○：MHLW, MEXT
(2) Addressing increasingly sophisticated and complex threats	◎：NISC, MIC, MEXT, METI ○：Other Ministries and Agencies
(3) Pursuing government agency initiatives	◎：NISC, NPA[*1], MIC, MOD ○：Other Ministries and Agencies
4.4.3 Collaboration based on full participation and awareness raising	◎：NISC, MIC, METI ○：Other Ministries and Agencies
5. Implementation Framework	◎：NISC, CAS ○：NPA[*1], FSA, MIC, MOFA, MOF, MEXT, MHLW, METI, MLIT, MOD, Other Ministries and Agencies ※CAS：CCS, NSS

***Organization Name Key**

CAO	Cabinet Office
CAS	Cabinet Secretariat
CCA	Consumer Affairs Agency
CCS	Assistant Chief Cabinet Secretary (Situations Response and Crisis Management)
CIRO	Cabinet Intelligence and Research Office
DA	Digital Agency
FSA	Financial Services Agency
MAFF	Ministry of Agriculture, Foresty and Fisheries
METI	Ministry of Ecomony, Trade and Industry
MEXT	Ministry of Education, Culture, Sports, Science and Technology
MHLW	Ministry of Health, Labour and Welfare
MIC	Ministry of Internal Affairs and Communications
MLIT	Ministry of Land, Infrastructure, Transport and Tourism
MOD	Ministry of Defense
MOE	Ministry of the Environment
MOF	Ministry of Finance
MOFA	Ministry of Foreign Affairs
MOJ	Ministry of Justice
NPA*1	National Police Agency
NPA*2	National Personnel Authority
NISC	National center of Incident readiness and Strategy for Cybersecurity
NSS	National Security Secretariat
SPPC	Specific Personal Information Protection Commission

The Government of Japan