1. Introduction

1.1. A Paradigm Shift Brought About by Cyberspace

Cyberspace, with the Internet as a central part of its platform, rose out from the rapid development of digital technology based on modern scientific knowledge, and has continued to expand and develop globally due to the autonomous initiatives of multiple stakeholders,[1] many of which operate in the private sector.

As a result of its development, cyberspace has allowed information and data, diverse in terms of both volume and quality, to be freely created, shared, and analyzed across national borders, unfettered by either time or space. Thus, cyberspace actors can potentially generate new value by interacting with fellow actors.

As a result of these characteristics, cyberspace is a place in which intellectual property, such as technological innovations and new business models can be created, and will continue to serve as a platform for sustainable development of economic society. This space also supports liberalism, democracy, and cultural development, as well as a place where people can utilize creation and innovation to significantly expand their activities.[2] In other words, cyberspace is a "frontier for generating infinite value." Japan will use all means under its disposal to undertake cybersecurity initiatives in order to ensure that cyberspace remains this way.

In the near future, the further development of computer science for which cyberspace is a prerequisite, such as artificial intelligence (hereinafter referred to as "AI"), etc. is expected to lead to the creation of new products and services. The emergence of new products and services change peoples' awareness by changing their daily behavior and living environment, and this triggers the transformation of social systems and industrial infrastructures that include existing procedures, models, organizations, etc. As humanity experiences a paradigm shift from hunting society, agricultural society, industrial society, and information society to "Society 5.0,[3]" it is necessary to

---

1 Multiple stakeholders are defined as "the national government, local governments, CII Operators, and Cyberspace-related Business Entities" in Article 16 of the Basic Act on Cybersecurity. Article 7 of the same Act defines Cyberspace-related Business Entities as "Cyberspace-Related Business Entities (referring to those engaged in business regarding the maintenance of the Internet and other advanced information and telecommunications networks, the utilization of information and telecommunications technologies, or involved in business related to Cybersecurity; the same applies hereinafter)."

2 In the Cybersecurity Strategy report (September 2015), the impact of these characteristics on society is compared to the explosion of knowledge triggered by Gutenberg's invention of letterpress printing.

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

examine the future vision of cybersecurity whilst taking into consideration these transformations.

1.2. Changes Since 2015

The Cybersecurity Strategy (hereinafter referred to as the "Strategy 2015"), enacted by the Cabinet decision in September 2015 after deliberations by the Cybersecurity Strategic Headquarters (hereinafter referred to as the "Headquarters") according to the Basic Act on Cybersecurity[4] (hereinafter referred to as the "Basic Act") was created as basic policy on cybersecurity-related measures covering a period of three years.

Following the formulation of the Strategy 2015, legal foundation for the utilization of data was prepared, including the Basic Act on the Advancement of Public and Private Sector Data Utilization[5] and the Amended Act on the Protection of Personal Information,[6] etc. The Government has also adopted a policy of realizing an anthropocentric society[7] that achieves both economic development and resolution of social issues through the high level of integration of cyberspace with real space. Under these circumstances, massive amounts of data generated by sensors and devices in real space are currently being accumulated and analyzed in cyberspace. Furthermore, the provision in real space of new products and services that adds value through use of data can be seen cyclically emerging and developing in numerous domains. No longer does cyberspace and real space exist as independent entities, but as mutually interacting entities, such that they cannot be considered separate anymore. Therefore, the two spaces should be seen as a single continuously evolving organic entity.

The unification of cyberspace and real space significantly increases the potential for affording abundance to society. At the same time, it also increases the opportunities for malicious actors to abuse cyberspace. The risk of economic and social loss or damage in real space is expected to expand and accelerate exponentially.

Under these circumstances, the security of cyberspace, which serves as the foundation of economic society, must be ensured, and at the same time, its autonomously sustained evolution and

4 This Basic Act was enacted on November 6, 2014. It afforded a legal position for the concept of cybersecurity and clarified the responsibilities of the various stakeholders.

5 This Act was enacted on December 7, 2016. It stipulates basic principles on the promotion of private sector data utilization.

6 This revised Act was enacted on September 3, 2015, and came into full effect on May 30, 2017. This Act was established to promote anonymization as a precondition before the utilization of personal information.

7 Contents of Society 5.0 (Source: Comprehensive Strategy on Science, Technology and Innovation 2017 (Cabinet Decision on June 2, 2017), Investment for the Future Strategy (Cabinet Decision on June 9, 2017).

development has to be ensured in order to achieve sustainable progress and wealth to society, Recently, there has been a trend for certain nations to respond to cyber threats by emphasizing management and control by the state from a dominant position. However, the strengthening of management and control of cyberspace by the state has the effect of hindering the possibility of autonomous and sustainable development. Thus, the cyberspace of today that developed through the autonomous initiatives of all stakeholders must be respected, and cybersecurity must be secured through collaborative and cooperative initiatives with those stakeholders.[8]

Based on this understanding, mindful of the state of affairs to be pursued for 2020 and beyond and taking into consideration the hosting of such international events as the Games of the XXXII Olympiad and the Tokyo 2020 Paralympic Games (hereinafter referred to as "the Tokyo 2020 Games"), Japan will spare no efforts regarding cybersecurity measures by clarifying the basic vision of cybersecurity, identifying new issues that need to be tackled; and swiftly implementing measures.

This strategy clarifies the basic position and approach to cybersecurity taken by Japan moving forward, while clearly indicating both domestically and internationally the goals and implementation policies of the various measures for the next three years in order to serve as the basis for shared understanding and action.

8 The "Sustainable Development Goals (SDGs)" adopted at the United Nations Summit in September 2015 established 17 goals for achieving a sustainable global society and a society in which "nobody is left behind." There are several points shared between the policy for cybersecurity initiatives here and the SDGs, such as aiming for sustainable development and initiatives based on the cooperation and collaboration between all stakeholders.

2. Understanding on Cyberspace

Knowledge, technologies, and services in cyberspace, such as AI, IoT,[9] Fintech,[10] robotics, 3D printers,[11] and AR/VR,[12] are becoming established in society and leading innovations that are transforming the existing structures in socio-economic activities and the daily lives of Japanese people, and these transformations are bringing about progress in the unification of cyberspace and real space.[13]

In order to create this strategy, an accurate understanding of the benefits afforded by cyberspace and the state of the threats in that space must be considered to be prerequisites. Furthermore, in order to enjoy the benefits of the knowledge, technologies, and services of cyberspace, it is essential to control the latent uncertainties always therein. When such control is not possible, the potential exists for cybersecurity related threats to increase rapidly.

2.1. Benefits of Cyberspace

Technologies and services in cyberspace are gaining routine use in numerous domains. The continued sustainable development of cyberspace is expected to bring about abundance for humanity.

(1) Advancements in Services in Cyberspace and the Adoption thereof by Society

The number of Internet users in Japan is rising, as has the spread of the Internet itself.[14] Furthermore, in terms of devices, the rate of personal smartphone ownership has increased significantly,[15] and the Internet usage rate is also rising.[16] The ratio of social media users is also rising,[17] as a result of which an environment now exists for easily communicating in cyberspace.

---

9 Abbreviation of Internet of Things.

10 A portmanteau combining the words finance and technology. It refers to new innovative financial services using new technologies such as the blockchain, big data, and AI, carried out through such devices as smartphones and tablets that have rapidly spread to wide adoption (Source: WHITE PAPER 2017 Information and Communications in Japan).

11 Compared to printers that output a flat (two dimensional) image to paper, a 3D printer forms three dimensional objects using three dimensional data from 3D CAD and 3D CG (Source: Website of the Japan 3D Printing Industrial Technology Association)

12 Abbreviations of augmented reality and virtual reality.

13 Strategy 2015 states that "physical objects and people in real space have become interconnected in a multi-layered manner without physical constraints, by harnessing the free flow of information and accurate data communications in cyberspace. Due to such linkages, there is an emergence of an "interconnected and converged information society" where real space and cyberspace have become highly integrated."

14 Internet penetration rate among the general population (82.8% as of the end of 2014 rose to 83.5% as of the end of 2016) (Source: WHITE PAPER 2017 Information and Communications in Japan)

15 Personal smartphone ownership rate (44.7% as of the end of 2014 rose to 56.8% as of the end of 2016) (Source: WHITE PAPER 2017 Information and Communications in Japan)

16 Internet usage rate (83.0% as of the end of 2015 rose to 83.5% as of the end of 2016) (Source: WHITE PAPER 2017 Information and Communications in Japan)

17 Trend in use rates for representative SNS services (LINE, Facebook, Twitter, mixi, Mobage, GREE) (total) (62.3% as of the end of

The increasing adoption of services in cyberspace by society has promoted not only the free flow of information, but also the formation of diverse communities and the sharing of information.

There has been progress in the area of financial activities as well, including online shopping, stock trading, and online banking, while new services in the areas of Fintech and the sharing economy[18] are appearing regularly and leading innovation. There has also been progress in the use of information and communication technology in medicine and nursing, welfare, education and other areas related to social issues such as the declining working-age population and the aging of local communities.

(2) Dramatic Evolution of AI

With respect to AI, there have been recent advancements in computer science, and in research on machine learning which requires massive quantities of data, giving rise to the new approach of deep learning. The emergence of deep learning has accelerated the optimization and increase in quality of numerous functions in socio-economic activities, including a significant increase in the precision of AI based image analysis, and increased precision in product anomaly detection, cancer diagnosis, investment decisions, and translation, and this technology is beginning to be adopted in a wide range of industries. Similarly, in the area of cybersecurity this potential of AI is also beginning to see use in the various measures such as the automation of malware detection.

The evolution of AI based on deep learning is said to be bringing about changes comparable to the Cambrian explosion in the world of machines and robotics.[19] Deep learning has enabled the design of feature extraction[20] used in differentiation and identification, a task that previously had to be carried out by a human in standard machine learning, to be carried out automatically by computers, and this is considered an evolutionary step for AI. Furthermore, a world in which AI is able to autonomously generate output resulting in creative works, such as music, paintings, and novels, and self-driving services (for example results from determination, decision making,

---

2014 rose to 71.2% as of the end of 2016) (Source: WHITE PAPER 2017 Information and Communications in Japan)

18 Economic revitalization activities in which personally owned assets that can potentially be used are made available for use by other individuals via online matching platforms (Source: WHITE PAPER 2017 Information and Communications in Japan)

19 The Cambrian explosion is the phenomenon by which the phylum of animals existing today arose suddenly between 542 million and 530 million years ago. Paleontologist Andrew Parker has presented the theory that the emergence of vision caused the explosion. Deep learning enables vision for AI. This enables AI to predict what will happen next and take action. Thus, it means the emergence of machines with eyes, and suggests that the equivalent of a Cambrian explosion will occur in the world of machines and robotics (Source: Headquarters for Japan's Economic Revitalization, the Fourth Industrial Revolution Conference to Promote Human Resource Development (2nd Meeting) Document 1)

20 A quantitative expression of the important characteristics requiring attention when recognizing an object. Before the arrival of deep learning, features were designed by humans. However, deep learning enables computers to carry out feature extraction on their own using image and sound recognition. (Source: WHITE PAPER 2017 Information and Communications in Japan)

and proposal) without any creative contribution by humans. The possibility has also been pointed out regarding who would be responsible if AI were to infringe rights or cause accidents.[21]

These developments in AI will lead to the emergence of entirely new products and services, and bring about changes in people's daily behavior and living environment in the future. This will cause changes in the way that humans perceive the world, which is expected to promote the transformation of existing social systems and industrial structures.

(3) Development of IoT

The reduction in size, weight, and cost of sensors has enabled an explosive spread in IoT, in which all things become connected to the network. In addition to the use of things such as home appliances, automobiles, robots, and smart meters, new businesses and services are being created to utilize the data obtained from IoT devices.

Specifically, efforts are being made to improve productivity and afford high added value in the areas of e-government, smart cities, manufacturing, self-driving automobiles, finance, health and medicine, and nursing,[22] and the utilization of data is expected to progress in the various supply chains[23] for those domains. Furthermore, there has been progress in so-called open innovation[24] in which cooperation occurs across domains via cyberspace, and new services are expected to emerge continuously that generate more abundance for people through the sharing and analysis of data.

2.2. Increasing Threats in Cyberspace

While AI and IoT technologies and services have the potential to bring many benefits to people, there is always the latent risk that the providers of these technologies and services will lose the ability to control them, in which case they can cause immeasurable economic and social loss or

21 "In the future, the problem might arise of whether users may be held responsible if the user (human) involvement with respect to the output of the AI product decreases." Intellectual Property Strategy Headquarters "Committee to Review Intellectual Property Regarding New Data-related Assets (Report)" (March 2017).

22 The Declaration to Be the World's Most Advanced Digital Nation / Basic Plan for the Advancement of Public and Private Sector Data Utilization (Cabinet Decision on June 15, 2018) defines eight priority fields (electronic administration; health, medical, and nursing care; tourism; finance; agriculture, forestry, and fisheries; manufacturing; infrastructure, disaster management, and disaster reduction; and mobility) expected to help solve issues such as (1) economic revitalization and the restoration of financial health, (2) regional revitalization, and (3) ensuring the safety and security of the lives of the people by promoting public and private sector data utilization.

23 The supply chain 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.

24 Open innovation refers intentionally and proactively utilizing the flow of internal resources, such as technologies and ideas, in and out of the organization to promote internal innovation, and deploying the resulting internal innovations outside the organization to increase market opportunities.

damage. As the unification of cyberspace and real space proceeds, the likelihood that such severe effects occur increase exponentially. Furthermore, cyberspace is a place unrestricted by space or time where anyone, including malicious actors, can misuse and abuse new information and communication technologies to act with ease. In addition to the ability for malicious actors and groups of such actors to easily copy and distribute data and information, including attack programs, which is due to the very nature of digital technology, they can also flexibly incorporate and make free use of developing technologies such as AI and the blockchain.[25] For that reason, the attackers have an asymmetrical advantage over the defenders, and that advantage is expected to increase particularly when the defender's formation depends on existing policies and technological systems.

Given these conditions, attacks[26] directed at IoT, Fintech including cryptcurrencies, critical infrastructure, and supply chains have occurred both inside and outside Japan, causing direct financial losses and the interruption of businesses and services in addition to the usual data breach, and serving to threaten the safety and security of the sustainable development of socio-economic activities and the people's living. There have also been massive incidents suspected to have been state-sponsored. There is also the concern that credibility of the information infrastructure may be shaken if a cyberspace is controlled and managed by some countries from a superior position.

It is believed that as cyberspace continues to become further unified with real space, there will be increased concerns over potential attempts to target weaknesses in IoT, supply chains, and open innovation, and for unintended behavior to occur in these systems. It is expected that serious impacts may occur not only for governmental bodies and critical infrastructure operators, but for other businesses and even individuals.

(1) Major Effects on Society Due to Interruptions to Business, Functions, and Services

Society will be significantly affected when interruptions occur to numerous businesses, functions, and services due to the interruption of important infrastructural services or unintended behavior by IoT devices, and situations could even develop to the point of becoming national security issues. If the unification of cyberspace and real space continues to progress further, contingencies may occur that threat the safety and security of the people and the very roots of democracy and the state, including the disabling of the functions of society and risks to human life and livelihood.

---

25 Referring to blockchain technology. It uses a data structure in which modification can be detected easily by using digital signatures and hash pointers. By storing the relevant data on multiple nodes distributed throughout the network, the technology achieves high data availability and integrity. (Source: Japan Blockchain Association, "Blockchain Definition")

26 The Bangladesh Bank was hacked, resulting in the unauthorized wiring of approximately 81 million dollars. A new type of malware (Mirai) emerged in September 2016, infecting IoT devices to cause the largest DDoS attack in history. A cyberattack also occurred on the transformer stations of a state operated power company in Ukraine in December 2016.

(2) Reduced Competitiveness Due to the Loss or Breach of Information

With the explosive spread in IoT and the increasing practice of making data publicly available, new services that use data will continue to increase in number. There will also be progress in the use of AI for data analysis. Data used for deep learning is directly related to the performance of the AI. As the importance of data continues to increase, damage to the authenticity[27] or integrity[28] of the data will undermine trust in the services that use the data.

In addition to being subject to claims for compensation for loss or damages, the data breach, such as personal information, trade secrets, and other valuable data, can also invite a fall in the reputation and trust an organization or company receives from society. Once breached, such data can never be taken back, and can lead directly to a drop in the competitiveness of the organization or company.

(3) Loss from Financial Theft and Fraud

Incidents have occurred in which inadequacies in basic measures for cybersecurity have led to unauthorized access to virtual currency exchange operators and massive financial damages through business email compromise. As socio-economic activities are expected to grow more and more dependent on cyberspace, inadequacies in cybersecurity measures are predicted to directly cause and expand financial damages and losses.

27 A characteristic that ensures an actor or resource is as claimed.

28 The information has not been damaged, modified, or deleted.

3. Visions and Objectives of this Strategy

The visions and objectives of this Strategy are clarified below as the firm maintenance of Japan's basic position on cybersecurity, and in light of such position, "the basic vision of cybersecurity" under the current understanding of cyberspace and its future image.

3.1. Adherence to the Basic Position on Cybersecurity

Japan will adhere to its basic position on cybersecurity including the "objectives of the Basic Act on Cybersecurity" and the "basic ideas and principles" presented in the Strategy 2015. On that basis, in order to continue to deter malicious actors' activities and guarantee people's safety and rights, Japan retains, as its options, political, economic, technological, legal, diplomatic, and all other viable and effective means.

(1) Objectives of the Basic Act on Cybersecurity

The Basic Act aims to "improve socio-economic vitality and sustainable development," "building a safe and secure society for the people," and "contributing to peace and stability of the international community and national security.[29]" This strategy also arranges policy goals within these three areas in order to promote measures accordingly.

(2) Basic Ideals

The basic ideals to which Japan will adhere to contribute to the objectives of the Basic Act is to aim for a "free, fair and secure cyberspace." Such a cyberspace means a secure cyberspace in which the freedom of expression and economic activities of all actors active therein is guaranteed without any discrimination or exclusion with no justifiable reasons, and where unlawful activities such as the theft of information or assets are not allowed.

(3) Basic Principles

The five principles stipulated by the Strategy 2015 as the basic principles to adhere to for developing and implementing cybersecurity measures are: (i) assurance of the free flow of information; (ii) the rule of law; (iii) openness; (iv) autonomy; and (v) collaboration among multi-stakeholders.

29 Article 1 of the Basic Act stipulates that "the purpose of this Act is to comprehensively and effectively promote the cybersecurity policy ... and as a result, attempting to enhance economic and social vitality, sustainable development and realizing social conditions where the people can live with a sense of safety and security, and contributing to the protection of international peace and security as well as national security."

(i) Assurance of the Free Flow of Information

For the sustainable development of cyberspace as a place for creation and innovation, it is imperative to build and maintain a world in which transmitted information reaches the intended recipient without being unfairly censored or illegally modified en route.[30] Consideration for privacy must also be maintained. As a basic condition for the free flow of information in cyber space, morality and commonsense are requested not to offend rights and interests of others.

(ii) The Rule of Law

As the unification of cyberspace and real space progresses, the rule of law should also be maintained in cyberspace in the same way as in real space. Various domestic rules and norms, including domestic laws and regulations, are applied in cyberspace. Similarly, existing international law is also applied in cyberspace. Application of existing international law and development of norms continue to be essential for sustainable development of cyberspace as a safe and reliable space.

(iii) Openness

In order to achieve the sustainable development of cyberspace as a space to generate new values, cyberspace must be open to all actors without restricting possibilities of linking diverse ideas and knowledges. Japan adheres to the position that cyberspace must not be exclusively dominated by some a certain group of actors therein.[31]

(iv) 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. The only approach to deter and address malicious actors' behavior to maintain order in cyberspace is for various social systems to achieve their missions and functions autonomously. The Government will promote this approach.[32]

(v) Collaboration among Multi-stakeholders

Cyberspace is a multi-dimension world established through activities of multi-stakeholders,

30 Article 1 of the Basic Act stipulates "to ensure the free flow of information ... simultaneously."

31 Article 3 of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society stipulates that "every people has an opportunity to easily and independently use the Internet and other advanced information and telecommunications networks."

32 Article 3 Paragraph 2 of the Basic Act stipulates that "The promotion of the Cybersecurity policy must be carried out with the intent to raise awareness to each member of the public about Cybersecurity and encourage each member of the public to take voluntary actions."

including the state, local governments, critical infrastructure operators, cyber-related and other businesses, education and research institutions, and individuals. For the sustainable development of cyberspace, all actors are required to consciously fulfill their respective roles and responsibilities. To do so, coordination and collaboration is required in addition to individual efforts. States have the role of promoting this coordination and collaboration, and will promote measures enabling the fulfillment of such roles.[33]

3.2. Basic Vision of Cybersecurity as a Goal

Based on Japan's idea mentioned above, the following presents the desired outcome that cybersecurity initiatives must aim for and three approaches required to promoting such initiatives as the "basic vision of cybersecurity."

(1) Goal

Japan aims to realize a society[34] in which cyberspace develop sustainably as "frontier generating infinite values," where new values and services are generated continuously, bringing abundance to the people.

In order to contribute to the realization of such society, cyberspace must develop through participation of all actors in generating new values. To support this sustainable development, all actors are required to be aware of their own roles with regard to cybersecurity and implement cybersecurity approaches autonomously, just like the immune systems of living things.

With such perspectives, the government will implement the following initiatives in order to promote cybersecurity initiatives.

Specifically, we will promote public and private sector initiatives on cybersecurity based on three approaches (1. mission assurance of service providers; 2. risk management; and 3. participation, coordination and collaboration) with the aim of autonomous and sustainable evolution and development of reliable cyberspace while realizing both security and economic development in cyberspace.

The image of cyberspace evolving this way through autonomous initiatives of all stakeholders mutually impacting each other will be called the "Cybersecurity Ecosystem" as compared to a

33 Article 3 Paragraph 1 of the Basic Act stipulates that "(Cybersecurity policy) must be carried out with the intent to produce active responses to threats against Cybersecurity through coordination among multiple stakeholders."

34 This refers to Society 5.0 (Sources: Comprehensive Strategy on Science, Technology and Innovation (STI) for 2017 (Cabinet decision on June 2, 2017), Growth Strategy 2017 (Cabinet decision on June 9, 2017)).

type of ecosystem that develops sustainably.

(2) Three Approaches

(i) Mission Assurance for Service Providers

Reliable execution of operations and services

"Mission Assurance" 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 execution such "missions." As part of that assurance, it is vital, from the standpoint of each organization carrying out their operations or services as "missions," for those responsible in each organization to proactively work towards securing cybersecurity without relying on some experts.

In other words, 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.

(ii) Risk Management

Assessment of Uncertainty and Appropriate Response

"Risk management" means to minimize risks to an acceptable level by identifying, analyzing, and evaluating risks[35] associated with "missions" assigned to organizations. The innate uncertainty of cyberspace unavoidably leads to this viewpoint.

Risk is defined as "the effect of uncertainty on objectives,"[36] and measurable only by considering the established objectives. Therefore, evaluation of or response to risks differs depending on objectives of the organization. Furthermore, risk management is defined[37] as "coordinated set of activities and methods that is used to direct an organization and to control many risks that can affect its ability to achieve objectives," and thus represents the overall set of activities of addressing risks through directing and controlling organizations and appropriately distributing organization's limited resources, which is not the individual activities of identifying, analyzing or evaluating risks.

35 Note that this refers to uncertainty that has both positive and negative aspects.

36 Definition given by the International Organization for Standardization (ISO)

37 Definition given by the International Organization for Standardization (ISO)

If each organization underestimates risks without acknowledging operations or services which represent its "mission" and does not allocate necessary resources to cybersecurity, it may lead to contingencies that can threaten the very survival of the organization. On the other hand, if the risks are overestimated and excessive resources are allocated to cybersecurity, it could impede the execution of organization's operations or services and its sustainable growth.

Such an approach to risk management is necessary for all, even individuals, who enjoy the benefits of utilizing knowledges, technologies or services of cyberspace.

When enjoying benefits, it is common for risks of losing control of prerequisite technologies or services to emerge. Accordingly, since mechanical prediction does not hold, and it is impossible to eliminate the risk completely, we need to properly address such risks according to the nature or manifestation of each risk, and minimize cybersecurity risks at an acceptable level in counterbalance with the merits of services and products provided thereof.

(iii) Participation, Coordination, and Collaboration

Measures, coordination and cooperation by individuals and organization from peacetime

"Participation, coordination and collaboration" applies to fundamental initiatives implemented by individuals or organizations from peacetime to prevent damages or its escalation possibly caused by threats in cyberspace. Any actor operating in cyberspace may potentially create new values as their benefits, but they may also be exposed to threats emerging from inherent risks. From this standpoint, it is necessary for not only organizations providing services but also individuals to take day-to-day basic cybersecurity efforts from peacetime.

Specifically, this includes measures to protect against malicious programs, mitigate vulnerabilities,[38] secure reliability of certifications, and manage personal information properly, among other things. These initiatives are often compared to public hygiene activities or transportation safety campaigns carried out in real space.

However, while cyberattacks may occur anytime or anywhere and threats become a daily concern, it is difficult to respond through individual efforts alone, and proactive support by other stakeholders including organizations, is required to strengthen such initiatives.

For this reason, it is necessary for everyone to work on initiatives together, which means they must cooperate. In addition to working on individual initiatives, it is necessary for every individual or organization involved in cyberspace to share information and mutually coordinate

38 People, things, and flaws in services that trigger threats.

and collaborate between each other regardless of peacetime or emergency situations. These basic cybersecurity efforts should be regarded as new cyber hygiene.

Accordingly, we need to support through public-private partnership to promote such fundamental initiatives. Particularly, under the principle of "collaboration among multi-stakeholders" listed under the Basic Principles, Japan must proactively carry out the role of promoting collaboration and coordination on a daily basis.

4. Policy Approaches towards Achieving the Objective

The following are the targets and guidelines of the policies scheduled to be implemented in the coming three years, for delivering results of the strategy. Each policy is expected to be consistent with the following three approaches described in Japan's Idea on Cybersecurity and the Basic Vision of Cybersecurity.

4.1. Enabling Socio-Economic Vitality and Sustainable Development

Enterprises are improving productivity of their business with active use of digital devices, such as personal computers and smart phones, and the Internet. Such technologies are also utilized to introduce business innovation, leading-edge services, and other new values. Cybersecurity measures should be regarded as "investments" as the basis to drive those trends, rather than unwanted "costs." Consistent cybersecurity measures bring about industrial growth and global competitiveness, and are critical for Japan's socio-economic vitality and sustainable development.

4.1.1 Advancing Cybersecurity as Value Creation Driver

Enterprises will face even higher cybersecurity risks along with the integration of cyberspace and real space. Cybersecurity awareness is increasing among a few industrial sectors and larger enterprises. Going forward, it is necessary in all industrial sectors to spread the understanding that cybersecurity initiatives must be carried out to ensure corporate business continuity and create new value, and to promote those initiatives.

In doing so, it is important to understand that cybersecurity related risks are one type of risks enterprises are facing and that measures should be handled as part of risk management. In addition, these measures should take root in organizations naturally according to the situation of each industry and business.

(1) Raising Executive Awareness

It appears the majority of business leaders are still obsessed with an idea that cybersecurity measures bring no profit for their business. This belief may come from an idea that cyberattack preparedness is nothing more than an unwanted "cost," since cyberspace is supposed to be offered for free without any precaution, and that cyberattacks to damage their business seldom happen. As the use of cyberspace grows rapidly, however, enterprises should understand that threats exist precisely because of this freedom and be prepared against them. Enterprises may find cybersecurity measures are difficult to adopt without organization-wide discussion to define their importance. Raising executive awareness is essential as they are expected to play

evangelistic role in penetrating thoughts that cybersecurity measures are indispensable investments for ensuring business continuity and value creation, but not inevitable costs.

Specifically, senior executives are expected to actively engage in cybersecurity through executive meetings and should acquire a certain level of knowledge and skills for risk management in cybersecurity affairs. However, requiring in-depth technical knowledge and skills to senior executives may not be quite realistic. Therefore, enterprises need to secure human resources (or "strategic management level") who are capable to grasp cybersecurity risks in the contexts of management and business strategies, plan cybersecurity measures in line with executive policies, and lead both business and technical personnel. Senior executives should build up appropriate risk management schemes for the entire supply chain, covering both their own and contractor organizations. Senior executives also should be accountable to shareholders for benefits and risks of business enabled by cyberspace.

Given this situation, the government will work in cooperation with private sectors to discover and train personnel who are capable of explaining and discussing cybersecurity measures with senior executives while hosting seminars for senior executives to promote a change in thinking. The government will also promote policies to appeal the importance of cybersecurity measures to senior executives in an easy to understand manner. These policies include the encouragement of declarations regarding company initiatives and the development of tools to visualize measures to make comparisons with measures taken by similar companies. The government will also work with academia to organize various legal systems that enterprises should refer to when implementing their cybersecurity measures.

(2) Stimulating Cybersecurity Investments

Corresponding managerial incentives are important for ensuring companies to implement cybersecurity initiatives on a continuous basis. Specifically, a virtuous cycle is desirable in which cybersecurity risks and associated measures are made visible including those from a financial perspective, senior executives understand the state of affairs and study and implement further specific measures necessary, the market positively evaluates those initiatives as efforts that lead to more corporate value, and incentives for cybersecurity investment are continuously generated.

To this end, it is important for companies to actively disseminate and disclose information regarding their cybersecurity initiatives. The government will share information on best practices and create guidelines while working on the continuous grasping and evaluation of the state of information dissemination and disclosure. In addition, it is necessary to go forward on the

creation of a framework for investors to evaluate cybersecurity initiatives from corporate management.

Regarding measures aimed at enterprises to promote cybersecurity, the government will follow up on the use of incentives for investment in cybersecurity so that they function effectively, and consider required measures as necessary.

Furthermore, the use of insurance is on the rise as a risk management approach to cybersecurity. This may make it easier to promote investment because the cost of preparing for risks will be clarified by the system in which insurance premiums are appropriately calculated according to the implementation status of cybersecurity measures. Based on this understanding, the government will consider measures for promoting the use of insurance in cybersecurity in cooperation with private sectors.

(3) Enhancing Cybersecurity Business Supporting Innovation Utilizing Advanced Technology

The use of advanced technologies, such as IoT, AI, VR, the blockchain, and next-generation telecommunications technologies, is often essential for enterprises to create new values. At the same time, the use of these technologies presents new vulnerabilities that previously did not exist, and malicious use of such technologies may also lead to unexpected risks. For that reason, there are expectations for realizing high quality products or services related to cybersecurity by estimating the risks beforehand and including cybersecurity measures in the processes of creating those products or services (security by design). Furthermore, these initiatives will lead not only to improved trust for Japan's products or services, but also to promoting the overseas deployment of high quality infrastructure that Japan is striving towards.

Meanwhile, due to a lack of expertise in cybersecurity, it may not be possible for enterprises to move forward with such initiatives easily despite their intent to do so. In addition, it is necessary from the perspective of enhancing international competitivity, and avoiding reliance on security products or services in which authenticity and reliability are difficult to verify. Therefore, there is a need to strengthen cybersecurity businesses that provide specific solutions domestically.

To meet these needs, the government will support the challenges towards new value creation using such advanced technologies not only by major enterprises but also venture enterprises. Specifically, the government will work in cooperation with private sectors to analyze and clarify cybersecurity risks associated with the use of advanced technologies and to prepare and disseminate guidelines based on such analysis and clarification. In addition, the government will

promote research and development on risk analysis and threat countermeasures for advanced technologies required for these initiatives. It is important to place the concept of security by design at the foundation of these initiatives. The government will also deliberate the building of systems to match enterprises aiming to create new values using advanced technologies with providers of cybersecurity technologies or services that support the use of those advanced technologies.

Furthermore, in order to promote international adoption of Japan's products or services that have achieved high levels of cybersecurity, the government will promote the benefits of such products or services through sales promotion by top government officials and trade shows. It will also work on the development of a business environment that facilitates international adoption by taking strict action through international cooperation against measures inhibiting free trade in the name of cybersecurity.

4.1.2 Achieving a Supply Chain that Creates Values through Diverse Connections

As unification of cyberspace and real space accelerates, previously nonexistent trade between different industries and enterprises is occurring on a global scale as we move towards Society 5.0. Furthermore, diverse and fluid forms that go beyond the traditional supply train are emerging, such as the automation of trade. Given these new forms, cybersecurity issues that occur at the edge of these connections of supply chains have the potential to spread more broadly than before and cause massive negative effects not only to real space but to the entire socioeconomic activities. It is essential to be aware of these risks and to promote initiatives that take the entire supply chain into consideration.

(1) Formulating Cybersecurity Framework for supply chain risk

As the supply chain connections take more diverse and fluid forms, it is essential for ensuring cybersecurity to implement consistent measures for the overall supply chain. It is also expected that the quality of products or services will give rise to new value creation through these implementations.

Specifically, the government will work in cooperation with private sectors to clarify threats in the supply chain and formulate as well as disseminate frameworks that cut across industrial categories for implementing operational-level measures. In order for business operators including small and medium-sized enterprises to implement the measures easily, adequate consideration will be given to ensure that the contents of the guideline are both realistically feasible and easy to understand, in light of situation of their circumstances. It is also important

to ensure that business operators can be aware of the balance between risks and costs of countermeasures.

It is necessary to offer specific measures of each sector required for IoT devices or organizations with an awareness of connections, areas requiring protection, and differences in threats related to the supply chain in each industry sector. Furthermore, as the supply chain expands globally, it is necessary to reflect overseas trends in the development of relevant rules so that cybersecurity measures based on Japan's security frameworks will be recognized globally.

(2) Building a System to Confirm Cybersecurity in the Supply Chain

Securing the trustworthiness of the elements comprising the supply chain including devices being manufactured, the data generated and distributed in devices, and the services that use them is essential in securing cybersecurity for the overall supply chain. To that end, it is necessary for the government to work to clarify the requirements and build a system that generates trust by certifying that such requirements are met. Consequently each element will be created and distributed in a way that meets security requirements. It is also necessary for the government to work with the private sector to build a system to create and manage a list of devices and services for which trustworthiness has been proven so that suppliers in the supply chain can verify that trustworthiness when using devices or equipment. The government will also consider a system to verify traceability and a system to detect and prevent attacks on the generated trust itself so that these become continuous systems within the connections of the supply chain.

(3) Promoting Initiatives by Small and Medium-Sized Enterprises

When small and medium-sized enterprises suffer financial damages and decline in trust due to cyberattacks, impact on operations can be greater than for major enterprises. There are also concerns that small and medium-sized enterprises can be used as footholds for expanding the impacts of cyberattacks from the company to its business partners. Meanwhile, cybersecurity measures must be promoted with the understanding that small and medium-sized enterprises do not necessarily possess high level knowledge or skills in cybersecurity, and it may be difficult for them to adequately invest in cybersecurity.

For that reason, the government will prepare easy-to-understand case studies of cybersecurity measures for small and medium-sized enterprises that include models for the safe use of information systems, and will promote the use of insurance in cybersecurity. The government will also strengthen the consultation system for small and medium-sized enterprises on cybersecurity incidents. Furthermore, the government will promote visibility initiatives in

cooperation with private sectors for small and medium-sized enterprises working on cybersecurity to promote their efforts to the public on their own initiative. The initiatives will include a systems to enable them to carry out their cybersecurity efforts effectively coordinated with incentive programs.

4.1.3 Building Secure IoT Systems[39]

The number of devices connected to cyberspace is rapidly expanding, and cybersecurity measures for vulnerable things, which can negatively impact cyberspace as essential infrastructure for the development of socio-economic activities, has become an urgent issue. Furthermore, as connections grow between numerous things (IoT devices) with different safety standards, including security levels or physical security, those connections have the potential to generate new threats. Given this situation, the government must work with private sectors to build secure IoT systems.

(1) Improving Structural Framework for IoT Systems and International Standard

To date, the government has worked on cybersecurity measures for IoT systems together with private sectors by carrying out various initiatives for realizing secure IoT systems, including the creation of guidelines. Moving forward, it is necessary to place emphasis on value creation by secure IoT systems, and work strategically with an integral and consistent manner.

To that end, according to the basic elements[40] of cybersecurity required to realize secure IoT systems presented so far by the government, the government will cultivate a shared understanding among stakeholders of the basic principles, objectives, methods, and time limits of measures, and clarify roles and functions of each sector or stakeholder. In addition, the government will promote initiatives in which each stakeholder cooperates while promoting autonomous cybersecurity measures. Furthermore, to promote these initiatives, the government will work to visualize the issues and associated initiatives of each stakeholder in public and private sectors in a manner that provides an overall picture, and build a system for sharing information. These initiatives will include not only sector-specific issues weighing on the actors in the public and private sectors but also common issues such as their scope, definitions, physical safety measures, demarcation points of responsibility (including the legal responsibilities of each actor including product liability of the manufacturers and the safety management obligations of the operator, etc. for incidents concerning the response to known vulnerabilities), and privacy

[39] A system in which everything including home electrical appliances, automobiles, and smart meters are connected to the Internet and other networks, making it possible to provide new services by utilizing big data, etc. that it generates.

[40] General Framework for Secure IoT Systems (October 2016, Cybersecurity Strategic Headquarters)

issues. Furthermore, the government will work in cooperation with private sectors to promote efforts for international standardization of the basic elements of cybersecurity required for realizing secure IoT systems in order to develop value creation systems for IoT systems and deploy it on a global scale while utilizing Japan's strengths of safety and security in order to contribute to the development of the global economy through spreading such secure IoT systems.

(2) Preparing a Formation for Vulnerability Countermeasures

To handle the increasing seriousness of cyberattacks on IoT devices, it is important to implement measures to ensure security and trustworthiness of information and communication networks, under the coordination and division of roles between industry, academia, and the public and private sectors. For that reason, the government must work with private sectors to prepare a formation for cybersecurity measures that cover the entire lifecycle of IoT devices from design and manufacturing through operation to disposal, and for measures regarding vulnerable IoT devices on information and communication networks.

Cybersecurity measures for IoT devices that cover the entire lifecycle should be implemented with full consideration for how each device is used and the relevant cybersecurity threats to it and the state of overseas deliberations and technology trends and developments. In addition, these measures should be taken with the mutual understanding and coordination of all stakeholders such as IoT device providers, telecommunications carriers, and users. As part of this, the government will work with private sectors to list cybersecurity requirements for each IoT device based on its characteristics and encourage the use of IoT devices that meet such requirements.

Furthermore, regarding measures for vulnerable IoT devices on information and communication networks, the government will steadily improve necessary systems to survey and identify IoT devices that use flawed password and expeditiously warn users thereof by telecommunication carriers. In addition, when implementing measures, related ministries and government agencies will work together and coordinate with telecommunication carriers and device manufacturers.

In the future, the government intends to contribute to establishing a safe environment by improving global information and communication networks by taking these Japanese measures as models and expanding them overseas through international coordination and standardization.

4.2. Building a Safe and Secure Society for the People

For the realization of society in which the people can live safely and securely, it is important to ensure multi-layered cybersecurity, through the coordination of multi-stakeholders, including governmental bodies, local governments, cyber-related enterprises, critical infrastructure operators, educational and research institutions, and every people themselves.

In particular, operations and services provided by governmental bodies, critical infrastructure operators, industry associations, and local governments (hereinafter referred to as critical infrastructure operators etc.) form the foundation that supports smooth socio-economic activities and people's living. Given the understanding that it is impossible to completely eliminate risks of cybersecurity, the government will promote initiatives based on the "mission assurance" approach declared under the basic vision of cybersecurity in order to reduce risks to an acceptable level and ensure that these operations and services are provided safely and continuously.

Meanwhile, Japan is preparing for national and international sporting events such as the Rugby World Cup 2019 and the Tokyo 2020 Games, which can be expected to provide incentives for cyberattacks to malicious actors. Thus, it is necessary for each stakeholder to deal with each situation by steadily carrying out their respective roles and cooperating with each other to realize a smooth implementation of the Tokyo 2020 Games and other events while also looking further ahead to the future.

4.2.1 Measures for the Protection of the People and Society

With increasing threats to cyberspace, many people have developed a feeling of anxiety about cybercrime, leading to an increase in awareness of cybersecurity throughout the society. Given these conditions, it is essential for all stakeholders to autonomously raise their security awareness and work proactively while creating an environment where multi-layered cybersecurity is ensured in collaboration among stakeholders.

(1) Building a Safe and Secure Cyber Environment for Users

Because cybercrime and cyberattacks are becoming more sophisticated and complex, and types of attacks are diversifying, they can no longer be handled using traditional passive measures only, and more proactive measures than what were previously used must be implemented.

Given this situation, the government, cooperating with cyber-related enterprises, will promote the policy of "Proactive Cyber Defense[41]" that ensures the government to implement active

41 Initiative that defends proactively against cyberattacks.

preventive measures against threats in advance. Specifically, the government will work to promote such initiatives to prevent damages from cybercrime or cyberattacks such as promoting the sharing and utilization of threat information to enable preemptive defense, using technologies to induce attacks to collect information on attackers, and conducting measures against botnets.[42]

The government will also promote the development of dependable information infrastructure, including the reinforcement of international undersea cables and other infrastructure facilities, which will be the foundation of overall services provided by governmental bodies and critical infrastructure operators, etc. The government will consider how to verify the evaluation of trustworthiness and how to improve the practice of government procurement and press forward with measures.

Furthermore, the government will work with providers of cryptocurrency services to promote measures so that the people may safely engage in the trading of cryptocurrencies. Also, with regard to self-driving vehicles and drones, the government will promote measures to avoid the occurrence of unauthorized operations due to cyberattacks as they may cause risks to human life. With regard to self-driving vehicles in particular, the government will continue to take the lead in the ongoing debate in the international forums on the establishment of international standards for cybersecurity.

(2) Enhancing Measures against Cybercrimes

As cyberspace increasingly becomes part of people's living, cybercrime has become a serious social issue due to the occurrence of global scale damages from ransomware infections[43] and cases in which unauthorized transmission of large monetary amounts apparently was carried out against domestic cryptocurrency exchange operators by malicious actors. In order to ensure the safety and security of the people, the government will continue to work to grasp the actual state of cybercrime and promote a crackdown on such crime while cooperating with related institutions or organizations in carrying out public awareness campaigns getting each individual person to promote autonomous measures against cybercrime. Furthermore, improvement of investigative and technological capabilities is also essential for addressing new types of cybercrime.

To that end, the government continues to promote thorough investigative activities, consideration

42 Network that bundles together personal computers and other devices that have become completely manipulable by the attacker as the result of virus infection ("bots"). Used maliciously for such acts as DDoS attacks and spamming. (source: Information-technology Promotion Agency, Japan (IPA), Jouhou Sekyuritii Hakusyo 2017 (Information security white paper 2017))

43 A type of malware (short for malicious software) that encrypts data and then demands a ransom.

on new investigative techniques, and public awareness campaigns to prevent damages from cybercrime. 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. The government will also promote positive utilization of knowledge and experience of private enterprises, personnel exchange between public and private sectors, and countermeasures against cybercrime in which, in the light of information sharing, information analysis, prevention of damages due to cybercrime, and human resource development, public and private sectors collaborate each other.

In the event of cybercrime, it is necessary to ensure traceability in cyberspace for investigation. As cooperation with related business operators and international collaboration is essential for this, the government will implement any necessary initiatives for that purpose. Regarding the appropriate preservation of communications history data logs in particular, the government, on the basis of the relevant guidelines,[44] will get related business operators to take appropriate measure.

4.2.2 Protection of Critical Infrastructure through Public and Private Sector Cooperation

Regarding the protection of critical infrastructure, the government has implemented initiatives based on the set of five policy groups of the Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)[45] (hereinafter referred to as the "Cybersecurity Policy"), based on the concept of "mission assurance" to provide critical infrastructure services safely and continuously.[46] However, the issue remains that there are variations in the level of cybersecurity awareness and progress in initiatives between each critical infrastructure sector. In order to solve these issues, it is necessary to raise the overall level of cybersecurity. Accordingly, the government will work with private sectors to provide proactive support as each stakeholder works on its own autonomous initiatives, including the consideration of models for cybersecurity measures regarding critical infrastructure operators with limited management resources for which it is difficult to adequately invest in cybersecurity.

44 Explanation of the "Guidelines on the Protection of Personal Information in the Telecommunications Business."

45 Cybersecurity Strategic Headquarters Decision on April 18, 2017

46 These are the Maintenance and Promotion of the Safety Principles, Enhancement of Information Sharing System, Enhancement of Incident Response Capability, Risk Management and Preparation of Incident Readiness, and Enhancement of the Basis for CIP.

(1) Primary Initiatives Based on the "Cybersecurity Policy"

To date, the government has formulated and revised the "Cybersecurity Policy" for the protection of critical infrastructure, and it will continue to implement initiatives based on the "Cybersecurity Policy." The "Cybersecurity Policy" is scheduled for review following the Tokyo 2020 Games. However, it will be reviewed even prior to the scheduled date if necessary, if there are major changes in the direction of society.

Critical infrastructure sectors are designated from the perspective of particularly requiring protection in consideration of degrees of impact they have on people's living and socio-economic activities. In view of social conditions, the government will expand the scope of critical infrastructure sectors and operators to develop the scope of security initiatives and strengthen "protection as a plane," as necessary. At the same time, it will further promote initiatives to share information, and expand or enhance information sharing systems.

Furthermore, the active involvement of senior executives officials at critical infrastructure operators is essential to promote initiatives for protecting critical infrastructure. Accordingly, the government will reach out to the senior executives to raise their awareness of cybersecurity while promoting the following initiatives.

(i) Promotion of Risk Management

It is necessary to provide critical infrastructure services safely and continuously even during cyberattacks. For that reason, in addition to implementing security measures in advance, it is important for critical infrastructure operators to prepare business continuity plans (BCP) and contingency plans based on the concept of mission assurance, in light of the results of risk assessment with cross-organizational and complex risks in mind. The government will implement initiatives to ensure that these overall risk management activities function continuously and effectively.

(ii) Improvement and Promotion of Safety Principles

In order to promote appropriate handling by critical infrastructure operators, the government will work on further promotion of guidelines for the preparation of safety principles, while continuously promoting initiatives to improve those safety principles including the recommendation of methods for data management and reduction of risks due to human factors based on surveys on the current state of data management and relevant international trends, taking into consideration such matters as the content of the business, size of the organizations, the duration of system use, and the impact on international competitivity. Furthermore, from the

standpoint of maintaining safety, the government will appropriately improve the institutional frameworks by means such as positioning cybersecurity measures as safety regulations within related laws and regulations, etc.

(iii) NISC Cyber Incident Severity Scale for CIS Outages

According to recent trends in cyberattacks, it is necessary to enable stakeholders, such as governmental bodies and critical infrastructure operators, to quickly share their understanding and determine whether a rapid response is necessary when a cyberattack is detected. To that end, the government will prepare the "NISC Cyber Incident Severity Scale for CIS Outages" and evaluate and publish the severity of incidents to encourage and enable diverse stakeholders to respond rationally and appropriately while taking into consideration the effect and impact of thoroughly informing the public. The government will also review the Scale as appropriate to improve it.

(iv) Joint Training and Exercises between Public and Private Sectors

It is important to conduct training and exercises with the assumption of the occurrence of service outages to increase the capabilities of critical infrastructure operators so that they can respond to such situations appropriately. The government and related institutions will continue to implement training and exercises among stakeholders of various sizes across public and private sector boundaries, and expand the scope and improve the contents thereof as necessary for their continued development.

(v) Security Measures for Industrial Control Systems (ICS)

There are critical infrastructure operators in such sectors as electricity, gas, and oil that use industrial control systems (ICS) to provide services. In these cases, it is likely that normal service provision becomes impossible when such ICS are significantly affected by cyberattacks and the like, causing a major impact on people's living. Accordingly, public and private sectors will unite to promote human resource development regarding ICS and carry out collection, analysis, and deployment of threat information as appropriate so that adequate security measures based on the characteristics of ICS will be implemented for safe and continuous provision of services.

(2) Strengthening and Enhancing Security in Local Governments

The services provided by local governments are closely related to people's living, and any obstacles on the provision of those services can have a major impact on community activity. While there are limits to technical solutions that can be taken for cybersecurity measures individually by organizations with limited resources, it is first and foremost necessary to

implement countermeasures against the leak of information, including Indivisual Number, due to service interruption or human error.

Given this situation and while direct involvement[47] of the national government in local government is limited compared to other organizations due to the current division of roles between national and local governments, local governments nationwide have been undertaking the fundamental reinforcement of measures, and the national government will update its guideline on security policy as necessary in light of the necessity to achieve a high level of security. The government will also work to achieve the necessary security levels for operational networks and promote initiatives to secure and develop cybersecurity human resource, enhance systems as well as securing the necessary budget while being mindful of the need for smooth operations by local governments.

Furthermore, with regards to identity federation among public and private sectors, the government will work to improve the environment balancing between convenience and security.

4.2.3 Strengthening and Improving Security in Governmental Bodies and Government-Related Entities

To date, efforts have been made to raise the level of information security measures for governmental bodies overall through the development of information security measures based on unified standards, initiatives for auditing based on those standards and the monitoring of unauthorized communication, and the government is required to continue working on these initiatives. The framework for initiatives at Incorporated Administrative Agencies and Designated Corporations (hereinafter referred to as "Incorporated Administrative Agencies, etc.") has been expanded in the same manner as for governmental bodies through the revision of the Basic Act on Cybersecurity,[48] and it will be an important issue moving forward to promote effective information security measures at Incorporated Administrative Agencies, etc. in consideration of the characteristics of their diverse business forms.

Responding to increasingly complex and sophisticated cyberattacks, there is a need to use new technologies to overcome the existing state in which attackers have the advantage while strengthening defense in depth that assume attacks will occur and countermeasures for risks to supply chains.

47 Unification and auditing of technical specifications.

48 Enacted on April 15, 2016. Expanded the scope to cover the monitoring, auditing, and investigating the causes of unauthorized communications by the government.

The smooth execution of government services is an extremely important responsibility for governmental bodies and Incorporated Administrative Agencies, etc. (hereinafter referred to as "the Agencies"), and it is important to make the necessary IT investment and security-related investment together as one when making investments for their systems. In light of this situation, it is important to secure the funds necessary to amplify security-related investments by such means as using the funds generated by making IT investment by the Agencies more efficient for security, and to strengthen the information security measures described above.

(1) Advancing and Visualizing Security Measures for Information Systems

The Agencies will utilize new defensive technologies to carry out more effective initiatives, aiming not only to increase the response capability towards the growing threat of cyberattacks, but also to prevent damages and, in the case of the occurrence of damages, prevent its spread and minimize the damage.

(i) Increasing Defensive Capabilities and Conditional Awareness for Information Systems

The Agencies will work to prevent damage preemptively and prevent its spread thereof by detecting malware behavior at the endpoint (personal computer, etc.) where programs are run. By automation of IT asset management, the Agencies will monitor the state of information systems in real time and enable the rapid handling of software vulnerabilities. Data protection initiatives will also be carried out for all Agencies to prevent information leakage when incidents occur. Furthermore, it is necessary to examine measures for identifying attacks that are difficult to detect by analyzing threat, combining the phenomena that occur on various devices and account management information. In order to implement those measures effectively, systems with a view to automating the work required for analysis of information must be established.

(ii) Preventing Damages and the Spread Thereof through the Advanced Cross-Organizational Collaboration among the Agencies

With consideration for the implementation status of malware monitoring on devices and automation of IT asset management at all stages, including prevention, detection, recovery, and response, the Agencies will aim for the development of cross-organizational initiatives by sophistication of effective and efficient collaboration between the Agencies and the GSOC[49] which includes the appropriate sharing with the GSOC of information to be gained on such measures.

49 Abbreviation of Government Security Operation Coordination Team. This team carries out cross-organizational monitoring and rapid response for the information security of governmental bodies.

(2) Promoting Use of the Cloud for Effective Security Measures

So that each Agency can select an appropriate form of information system according to the characteristics of the information and that security measures can be carried out efficiently and effectively for the overall government, the government will promote the use of cloud services including migration to a government common platform in the form of a government private cloud that can utilize the benefits of consolidating the building and operation of systems and increasing the security level. In promoting the use of the cloud, the government will consider and go forward with measures to promote the use of a reliable cloud in which an appropriate level of security such as safety evaluation is secured.

With regard to the Internet connection lines, the government has also worked for the unification and consolidation of the connection port under the common standard. The government will make the necessary considerations including the consolidation of perimeter monitoring points while collaborating with government common networks and platforms, since the further promotion of the appropriate consolidation of Internet connection ports for governmental bodies is extremely effective for operations and security measures.

(3) Preemptive Efforts Utilizing Advanced Technology

Some of the information system platforms that have grown in use in recent years have a particularly high level of resistance to cyberattacks. The government will consider utilizing the information technologies created under this new design philosophy for the Agencies, work to accumulate knowledge of best practices, and aim for a shift towards defender's advantage.

(4) Raising the Cybersecurity Level through Auditing

In light of the Basic Act on Cybersecurity, the government will provide the trends and issues identified through the cross-organizational analysis of data from the auditing of the Agencies as feedback for the entire Agencies to promote the further raising of the cybersecurity level. In addition, the government will utilize the IT asset management information of the Agencies that is developed in accordance with initiatives in monitoring the state of those systems efficiently, and will aim for efficient and effective implementation of auditing.

(5) Improving Organizational Response Capability

Primarily via the team that handles incidents,[50] the government will increase incident response capability and information security knowledge of each Agency. In case of occurrences of cyberattacks to the Agencies, the government will enhance the training, etc. for coping capability

50 CSIRT (Computer Security Incident Response Team)

building of the staff in order to strengthen the mobile assistance formation (an emergency assistance team for information security)[51] which is comprised of government employees with requisite knowledge and skills of each government agency.

4.2.4 Ensuring a Safe and Secure Educational and Research Environment at Universities etc.

Universities and Inter-University Research Institutes etc. (hereinafter referred to as "universities etc.") are staffed by various members with a diverse collection of IT assets and systems in use. Given the nature of these universities etc., along with the implementation of autonomous cybersecurity measures by the universities etc. by themselves, it is important for the government to proactively support the building of response system and sharing of information etc. to deal with cyberattacks through collaboration among the universities etc. in order to ensure a safe and secure educational and research environment.

(1) Promoting Measures in Light of the Diversity of Universities etc.

The senior executives of universities etc. must personally understand the importance of cybersecurity measures, position cybersecurity measures as important managerial issues, and carry out initiatives as an organization based on a plan for promoting cybersecurity measures, while also conducting follow-ups to further promote cybersecurity measures.

In doing so, it is necessary to identify the IT assets to protect, evaluate the cybersecurity risks, and consider the managerial and technical measures to be prioritized when implementing in accordance to those risks, with consideration for the diversity of the universities etc. that conduct education and research in various areas. Furthermore, universities and research institutes also need to consider initiatives to improve the capability to respond quickly and appropriately to incidents, and a system to implement the measures organizationally and steadily.

The government will promote the autonomous and organizational initiatives of the universities etc. by creating and disseminating guidelines on cybersecurity; implementing practice for each level regarding risk management and incident response, and practical training and exercises, and support for the initial response to the event of incidents.

(2) Promoting Cooperative and Collaborative Initiatives by Universities etc.

Universities etc. use common information platforms and face similar cybersecurity issues. Strengthening of the cybersecurity measures in light of these actual conditions at the universities

51 CYMAT (Cyber Incident Mobile Assistant Team)

etc. is considered important, and there is a need for further promotion of initiatives through mutual cooperation of all the parties involved.

For this reason, organizations that operate science information networks will collaborate with national universities etc. to develop a system to monitor, detect, and analyze cyberattacks and provide information on those attacks, while also carrying out joint research and training for technical staff to maintain and strengthen the functions of monitoring capabilities and develop strategic management level, and training for technical staff.

In order to strengthen the incident response team at those universities etc., the government will also support initiatives that the incident handling team for multiple universities and research institutes shares information, common issues and knowledge for incident response related to cyberattacks.

4.2.5 Initiatives for the Tokyo 2020 Games and Beyond

Countless athletes, foreign dignitaries, and supporters will gather from all over the world for the Olympic/Paralympic Games, giving the hosting of the event the highest possible level of attention and potentially making it a target for cyberattacks.

Reflecting on the past Olympic/Paralympic Games, it has been reported that there was a massive number of cyberattacks during the London 2012 Games, though they did not affect the operation of the event. Similarly, according to some reports there was a significant number of cyberattacks causing damages to the Rio de Janeiro 2016 Games and the PyeongChang 2018 Games. The Tokyo 2020 Games is also expected to be subject to even more cyberattacks than in the past and, by their nature, some attacks will assumingly be targeting multiple service sectors. For that reason, the government will ensure cybersecurity for the Tokyo 2020 Games and promote further measures looking beyond the event.

These various measures will be expanded in scope and continued after the Tokyo 2020 Games, and the legacy of the systems developed, and experience and knowledge in their operation will be utilized to strengthen cybersecurity in Japan continuously into the future.

(1) Preparedness for the Tokyo 2020 Games

Based on the basic strategy[52] decided by the Security Board Meeting of the Headquarters for the Tokyo 2020 Olympic/Paralympic Games, the government will continue the collection of

52 The Basic Strategy on Security for the Tokyo 2020 Olympic/Pralympic Games (the Security Board Meeting of the Liaison Council of Ministries and Agencies Related to the Tokyo 2020 Olympic and Paralympic Games, March 21, 2017)

information concerning the safety of the Games and other measures. It will also carry out the assessment of cybersecurity risk sources taking into consideration the coordination with physical security, conduct the cybersecurity risk assessment of critical service providers that have the potential to affect the Tokyo 2020 Games operations including the consideration of risk scenarios based on the results of the assessment of cybersecurity risk sources, and promote measures for various risks including the cross-sectoral risks identified by the risk assessment. In addition to the sharing of information on cybersecurity threats among Olympic related organizations, such as the relevant ministries and governmental agencies, the Tokyo Organising Committee of the Olympic and Paralympic Games, the Tokyo Metropolitan Government, local governments providing venues, and critical service providers, the government will promote the development of the Cyber Security Incident Response Coordination Center (Government Olympic/Paralympic CSIRT), the organization through which the government takes a role to coordinate the Olympic related organizations so that they can respond to cybersecurity incidents together when an incident occurs, and work to ensure the preparedness for close communication and coordination.

(2) Passing on Results that Lead to the Future

The government will continue to promote the various measures in preparation for the Tokyo 2020 Games, and the systems developed, and the operational experience and knowledge of those systems will be utilized as a legacy to strengthen Japan's continuous cybersecurity after the Tokyo 2020 Games. Furthermore, the Cyber Security Incident Response Coordination Center will be utilized as an organization (national CSIRT) to serve as a coordinator and coordinating desk for all of Japan to work together to deal with cyberattacks. The methods for risk management described in the Basic Vision of Cybersecurity will be prepared and disseminated for wide application to business operators throughout the country.

4.2.6 Building an Information Sharing/Collaboration Framework that Extends beyond Traditional Frameworks

Essentially, the establishment of cybersecurity should be an initiative that each organization carries out autonomously according to the value of its data assets and the state of information and communication technology utilization. Meanwhile, due to the changes in attack modes, there has been a limit to the ability to put in place effective countermeasures against cyberattacks within a single organization. For that reason, an awareness is steadily spreading in both the public and private sectors that emphasizes collaboration with other organizations, and not only administrative organs and critical infrastructure operators, but also a wide range of other

stakeholders are beginning to work on information sharing.

As the number of sectors closely related to cyberspace further grows due to the increasing unification of cyberspace and real space, it is expected that the scope of sectors and stakeholders that need to share information contributing cybersecurity will continue to expand.

Accordingly, from the standpoint of "participation, coordination and collaboration" presented as part of the Basic Vision of Cybersecurity, the government must support existing initiatives for information sharing systems, such as ISAC,[53] through the close coordination between the stakeholders, while taking on new roles.

(1) Promoting Information Sharing and Collaboration between Multi-Stakeholders

With the increase in the number of stakeholders engaged in information sharing, the importance of the role of collecting and analyzing the information and coordinating the stakeholders in a timely manner also increases. In the meantime, because the inappropriate handling of the shared information has the potential to cause a decline in the social appraisal and trust, it remains an issue that the stakeholders are reluctant to proactively share the data they possess.

Given this situation, the government will work to build a new system that will enable multi-stakeholders in the public and private sectors, including specialized agencies with adequate knowledge and experience in information sharing, to share information contributing cybersecurity without anxiety. When doing so, it will be important to respect the autonomy of each stakeholder in accordance with the principle of autonomy presented in the Basic Principles. Information sharing and coordination that transcends public-private, industrial, national, and other boundaries between public and private sectors, industries, and the domestic and international will be promoted by implementing this initiative.

The government will also consider collaboration and unification between the multiple existing information sharing systems in the public and private sectors with consideration for the characteristics and roles of each of them so that the relevant parties shall not incur additional burden by new system.

(2) Towards a New Stage in Information Sharing and Collaboration

For the development of a new information sharing system, the government will consider a structure in which multi-stakeholders can build relationships of trust, and in which the more they

53 Abbreviation for Information Sharing and Analysis Center. This organization collects information on cybersecurity for analysis. The analyzed data is shared with ISAC members for use in their respective security measures. (Source: Cybersecurity 2017 (August 25, 2017))

actively collaborate and cooperate in providing information, the more they receive benefit from the system.

The more the level of collaboration and cooperation with other parties increases, the greater the benefits of participating in the information sharing system become. Accordingly, the government must take the lead in sharing the information in its possession appropriately. The government will also develop an environment in which stakeholders that proactively share their own information regarding such matters as cybersecurity incidents is positively regarded. In particular, it is essential that information regarding cybersecurity that causes recalls to protect the life and physical well-being of people is shared swiftly and surely. The government will also work to achieve appropriate and swift analysis and sharing of information truly needed by each stakeholder through the promotion of automatic processing of received information and other means.

Through this initiative, the understanding that the mutual sharing of information is essential to increase cybersecurity will be cultivated throughout society. Furthermore, having the sight set on the strategic collaboration with the international community is also essential, while developing Japan's information sharing system. The government will work closely with each stakeholder and work proactively towards improving the necessary environment to enable each stakeholder to build relationships for coexistence and mutual development that transcend the conventional sectoral boundaries associated with industries and the public and private sectors. This will enable the sharing of information and collaboration regarding cybersecurity to move ahead to a new stage.

4.2.7 Strengthening the Incident Readiness Against Massive Cyberattacks

Cyberattacks have occurred overseas and significantly impacted people's living, causing massive power outages or partial losses of functioning of financial institutions. As unification of cyberspace and real space continues, it is well within the realm of possibility for cyberattacks to cause incidents in real space in our country in the future. Furthermore, massive cyberattacks can be expected to cause simultaneous damages to services that are normally relatively unrelated, and the country must work as one to address risk management for threats in cyberspace to protect society and the people from those threats.

The government will carry out response training and exercises across both cyberspace and real space while strengthening the preparations to respond to cyberattacks through training and exercises in order to work on risk management for both cyberspace and real space. The

government will also promote training of personnel capable of analyzing cyberattacks, the sharing of information through a framework for public and private sector coordination, and the advancement of Internet monitoring in an effort to improve data collection and analysis capabilities and emergency response capabilities in cyberspace.

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

A free, fair, and secure cyberspace contributes to the peace and stability of the international community and to Japan's national security.

A cyberspace, which is open to all actors and where the autonomous and free flow of information is secured, fosters innovation and constitutes the foundation of democracy. Cyberspace has developed through technological innovations, inventions, and initiatives of multi-stakeholders in industry, academia, and the public and private sectors. Excessive control by states will impede the autonomous and sustainable development of cyberspace. For the sound development of cyberspace, multi-stakeholders need to cooperate to ensure the free flow of information, and maintain the openness and autonomy of cyberspace.

As the use of cyberspace accelerates throughout society, leading to the advancement of the unification of cyberspace and real space, the issues in real space, such as human rights, privacy, crime and terrorism, and national security, are brought into the realm of cyberspace and posing challenges. Accordingly, it is necessary to carry out initiatives with regard to these challenges to ensure the safety and security of cyberspace. Since cyberattacks can easily cross national borders and there are incidents that are suspected of being state-sponsored, it is necessary to promote the rule of law, increase defense, deterrence, and situational awareness capabilities against cyberattacks and promote international cooperation and collaboration in order to ensure the security and stability of cyberspace. However, when doing so, it is necessary to pay attention in order to avoid impeding the autonomous and sustainable development of cyberspace.

In order to safeguard a free, fair, and secure cyberspace, Japan will communicate its position in the international fora, ensure its national security by utilizing existing frameworks, and promote international collaboration.

4.3.1 Commitment to a Free, Fair, and Secure Cyberspace

In order to realize a free, fair, and secure cyberspace at the global level, Japan will communicate

its idea in the international fora and take an active role in promoting the rule of law in cyberspace.

(1) Communicating the Ideas of a Free, Fair, and Secure Cyberspace

In order to maintain the ecosystem of autonomously and sustainably developing cyberspace, Japan will aim to ensure the safety in cyberspace through the coordination and collaboration among multi-stakeholders on efforts to ensure cybersecurity, rather than through control and regulation such as controlling the flow of information by states.

Japan will communicate such basic approach to cybersecurity in the international fora. In addition, Japan will work with our ally and like-minded countries, as well as private entities to thwart any efforts that aim to inhibit the development of cyberspace such as through the change of international rules.

In doing so, it is necessary to separate discussions on how to manage Internet resources from discussions of the issues that arise through the use of cyberspace such as human rights, privacy, crime and terrorism, and national security. With regard to the issues that arise through the use of cyberspace, discussions need to be conducted under the premise of the existing frameworks.

(2) Promoting the Rule of Law in Cyberspace

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

Existing international law, including the Charter of the United Nations, applies to cyberspace also. Japan takes this position and will proactively contribute to discussions on the individual and specific applications of existing international law and the development and universalization of norms. Also, Japan will promote the universalization of norms of behavior of responsible states that have been apparent to date[54] by steady implementation and practice of such norms. Japan will deter any acts against such norms through the universalization of such norms in the international community and the accumulation of relevant state practices thereof.

With regard to measures against cybercrime, the National Police Agency and other relevant ministries and agencies will collaborate to further promote international partnership through international investigative cooperation and information sharing with international organizations,

54 These include the 2015 report of the fourth session of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), the 2015 G20 Antalya Summit Leaders' Communiqué, and the 2017 G7 Declaration on Responsible States Behavior in Cyberspace.

law enforcement agencies and security information agencies in foreign countries leveraging frameworks such as the Convention on Cybercrime, mutual legal assistance treaties, and the ICPO.[55]

Through these initiatives, Japan will promote the rule of law and realize the peace and stability of the international community and Japan's national security.

4.3.2 Strengthening Capabilities for Defense, Deterrence, and Situational Awareness

The security environment in cyberspace is growing increasingly severer. Cyberattacks have been taking place against governmental bodies, critical infrastructure operators, companies and academic and research institutions possessing advanced technologies. There are cases that might threaten to undermine the foundations of democracy. Furthermore, some of these attacks are suspected of being state-sponsored.

Given this situation, in order to protect the Japan's national security interests from cyberattacks, it is important to secure Japan's resilience against cyberattacks and increase Japan's ability to defend the state (defense capabilities), deter cyberattacks (deterrence capabilities), and be aware of the situation in cyberspace (situational awareness capabilities).

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 on a daily basis and proceed with the initiatives related to national security, under the overall coordination by the National Security Secretariat. When necessary, deliberation and decision will be made at the National Security Council.

(1) Ensuring National Resilience

(i) Mission Assurance

It is the mission of governmental bodies to protect and support people's lives and socio-economic activities. Any failure in playing their role is a significant concern for national security. The execution of the missions of these governmental bodies relies on the services provided by critical infrastructure operators and other business operators which maintain social system. These operators also have an important mission to provide these services indispensable for the people

55 ICPO is the Acronym for International Criminal Police Organization.

and the society.

Japan will promote the establishment of cybersecurity for governmental bodies and critical infrastructure operators in order to assure the execution of the missions of those governmental bodies related to national security and to provide services essential for the people and the society. As the defense authorities, in particular, the Ministry of Defense and the Self-Defense Forces, will continue to strengthen the defense of the networks and infrastructure on which their operations depend, while further enhancing the capabilities of cyber defense units against cyberattacks, and deepen collaboration with stakeholders involved in the mission assurance of the Self-Defense Forces.

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

Advanced technologies are important national assets not only for assuring economic advantage, but for national security as well. Japan will strengthen cybersecurity measures, including the reduction of human caused risks faced by the business operators and relevant ministries and governmental agencies that handle the technologies important to Japan's national security, such as technologies related to outer space, nuclear energy, security, and the defense equipment. Particularly, the leak or illegal disclosure of the technical information held by the defense industry would have a major impact on Japan's national security. For that reason, Japan will work to adopt a system to ensure the safe sharing of information, establish new information security standards for contractors, and revise contractual provisions. Deliberations will be carried out with the assumption that these measures will be applied to the entire supply chain for the defense industry, including subcontractors, through the collaboration between the public and private sectors.

Furthermore, the government will promote measures at national research and development organizations and universities and research institutes possessing advanced technology from the viewpoint of protecting information on advanced technologies.

(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 now serves as 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 externism, recruiting into the organizations, and gathering funds for organizations. For that reason, the government will strengthen the collection and analysis of information on the activities of terrorist organizations in cyberspace and take any

other necessary measures in collaboration with the international community, while also guaranteeing the basic human rights including the freedom of expression.

(2) Enhancing Deterrence Capabilities

(i) Measures for Effective Deterrence

International law, including the Charter of the United Nations, applies to cyberspace. As G7 leaders affirmed at the Ise-Shima Summit, under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of international law.[56] Also, as G7 foreign ministers affirmed at Lucca, among other lawful responses, a State that is the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures against the State responsible for the wrongful act.[57]

Based on the above-mentioned recognition, in order to deter malicious cyber activities and protect the people's safety, security, and rights, in close coordination with our ally and like-minded countries, Japan will utilize political, economic, technological, legal, diplomatic, and all other viable and effective means and capabilities, depending on the threat, and take resolute responses against cyber threats that undermine our national security, including those possibly state-sponsored.

The government will strengthen the coordination system among relevant governmental bodies with the Cabinet Secretariat as its core in order to make timely and appropriate responses, promote as a whole inter-agency and cross-sectoral efforts in a comprehensive manner, and the government will also strengthen capacity at the relevant authorities including law enforcement authorities and the Self-Defense Forces. In this regard, the acquisition of capabilities to prevent malicious cyber actors from using cyberspace may be considered.

(ii) Confidence Building Measures

The government will work to build confidence among states in order to prevent the occurrence of unforeseen circumstances and deterioration of the situation caused by cyberattacks. Due to

---

56 G7 Principles and Actions on Cyber (May 2016) "We affirm that under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law. We also recognize that states may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace."

57 G7 Declaration on Responsible States Behavior in Cyberspace (April 2017) "We note that, in the interest of conflict prevention and peaceful settlement of disputes, international law also provides a framework for States' responses to wrongful acts that do not amount to an armed attack - these may include malicious cyber activities. Among other lawful responses, a State that is the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures, including measures conducted via ICTs, against the State responsible for the wrongful act in order to cause the responsible State to comply with its international obligations"

the the anonymity and secrecy of cyberattacks, there are risks that cyberattacks unintentionally increase tentions among states and worsen the situation. In order to prevent such accidental and unnecessary confrontations, it is important to build up international communication channels 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. The government will also cooperate with other states to consider a mechanism for coordinating issues regarding cyberspace.

(3) Strengthening Cyber Situational Awareness

(i) Increasing the Capabilities of Relevant Governmental Bodies

In order to deter increasingly serious cyberattack, in addition to enhancing response capabilities, adequate capabilities to detect, investigate, and analyze cyberattacks are necessary to make the attackers accountable. To this end, the government will quantitatively and qualitatively improve the information collection and analysis capabilities of the relevant governmental bodies. Accordingly, the government will proceed with wide ranging considerations of any effective means including the development and securement of a cybersecurity human resource 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.[58]

(ii) Threat Information Sharing

Information sharing among relevant ministries and agencies within the government and with our ally and like-minded countries is essential for accurately responding to and deterring diverse threat of cyberattacks, including those suspected of state-sponsored and by non-governmental organizations. Accordingly, the government will promote the sharing of threat information with our ally and like-minded countries. 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

Because the effect of incidents in cyberspace can easily extend beyond national borders, cyber incidents in overseas can always affect Japan. Japan will cooperate and collaborate with the governments and private sector worldwide to ensure the security of cyberspace and work

58 Intelligence defense activity against hostile intelligence activity by foreign countries using information and communication technology

towards both the peace and stability of the international community and the national security of Japan.

To this end, the government will proactively contribute to various international discussions and work for the sharing of information and development of common understanding regarding cyber related issues. The government will also share expertise with foreign countries, promote specific cooperation and collaboration, and take actual action. Furthermore, we will secure and train personnel in the public and private sectors who are capable of expressing our position to the international fora.

(1) Sharing Expertise and Coordination Policy

The government will work through bilateral dialogues and international conferences on cybersecurity to exchange information on cybersecurity policies, strategies and system to respond, and utilize that knowledge in planning Japan's cybersecurity policy. We will also strengthen its cooperation and collaboration regarding cybersecurity policy with strategic partners that share basic principles on cybersecurity with us.

(2) International Collaboration for Incident Response

The government will share information on cyberattacks and threats and strengthen cooperation between CERTs[59] to enable the coordinated response when incidents occur. The government will also work to improve coordinated response capabilities through joint training and participation in international cyber drills and joint training. Furthermore, the government will respond appropriately in the case of incidents through appropriate international collaboration.

(3) Cooperating for Capacity Building

Today, as interdependence across borders has deepened, it is not possible for Japan to its secure peace and stability only by itself. Global coordination to reduce cybersecurity vulnerabilities and to aim for their elimination thereof is essential in contributing to ensuring Japan's national security.

From this standpoint, assisting capacity building in other state ensures the stability of the lives of Japanese residents and the activities of Japanese companies in other countries that depend on critical infrastructure in those states as well as the sound development of the use of cyberspace there. At the same time, it is also directly connected to ensuring the security of all cyberspace and contributes to the improvement of the security environment for the entire world including

59 The Computer Emergency Response Team (CERT) is an organization that responds to computer security incidents.

Japan.

According to the Basic Strategy on Cybersecurity Capacity Building for Developing Countries[60] published in 2016, the government will proactively promote capacity building in developing countries.

4.4. Cross-Cutting Approaches to Cybersecurity

In order to achieve the three policy goals – "enabling socio-economic vitality and sustainable development," "building a safe and secure society for the people," and "contribution to the peace and stability of the international community and Japan's national security,"- it is important to work on human resource development and research and development as a foundation for the policy goals from both a cross-cutting and mid- and long-term perspective. Simultaneously, it is also crucial to promote a cooperative approach in which everyone plays a role in working on cybersecurity as an active agent in cyberspace.

4.4.1 Development and Assurance of Cybersecurity Human Resource

The threat of cyberattacks is spreading as new value is being created towards the realization of Society 5.0, and it is necessary that each stakeholder take the initiative and play their respective roles rather than relying on the efforts of few experts to ensure cybersecurity.

In preparation for the future relevant to this coming paradigm shift, there is a need to clarify the level of knowledge and skill required of personnel involved in establishing cybersecurity from the standpoint of supporting each organization to carry out its mission and the safe use of cyberspace. Following this, it is necessary to form a virtuous circle in which the supply and demand for personnel is appropriated by: adequately treating personnel with good knowledge and practical abilities, certified by qualifications and evaluation standards obtained through education and; further enabling them to hone their skills through repeated practical experience.

To that end, the government will work with industry, academia, and the public sector to share information on the demand for personnel and measures regarding human resource development in order to strengthen the development and assurance of the cybersecurity human resource. In doing so, it is important to ensure the diversity of personnel from the standpoint of promoting innovation.

(1) Training and Adoption at the Strategic Management Level

In order to push forward cybersecurity measures as a part of company management, it is

60 Basic Strategy on Cybersecurity Capacity Building for Developing Countries (October 2016, Cybersecurity Strategic Headquarters)

inappropriate to leave the task up to experts and operational level staff because cybersecurity is not simply a technical issue.

Under the management strategies and business strategies that the senior executive management presents, the personnel capable of meeting this challenge must:

(i) understand the cybersecurity-related risks that must be assumed in conducting operations and services as part of the risks that an organization must manage; and

(ii) utilize and command operational-level staff experts to execute countermeasures and responses to incidents in the role of providing the core support for risk management regarding business continuity and value creation

Accordingly, the government will define the personnel taking on these roles as the "strategic management level" and work for the adoption of this concept through collaboration with industry, including the promotion of understanding among the senior executives.

There are also cases where, due to differences in culture or custom within industries or business categories, it may be difficult to integrate and implement cybersecurity measures into existing management systems for realizing operations and services. For that reason, the government will, while taking into account consider that there are many ways of business and management, and the government will promote the implementation of relearning programs, by means of the development of practical learning materials for the strategic management level and the identification and training of instructors.

(2) Training for the Operational and Expert Level

As for the operational and expert level who implement the measures regarding system planning, building, and operation, based on the instruction expressed by the strategic management level, numerous educational programs, certification and testing programs, and training have been carried out through public and private sector cooperation.

It is necessary to continue to strengthen such initiatives to raise knowledge- and skill-levels. Operational and expert level staff should also deepen their understanding of the information and communication technologies, control system technologies and cyberattacks that evolve on a daily basis. In addition, it is important in responding to these attacks that they understand the policies of senior executive management and function as part of a team, communicating with other expert level personnel. To do so, it is necessary to use development programs for operational and expert levels to develop skills for understanding the conceptual and abstract

ideas presented by the strategic management level and converting them into concrete measures while engaging in smooth communication with a variety of stakeholders.

The government will also continue to identify, train, and assure personnel with exceptional abilities who are capable of competing on the global stage. For example, the government will continue to promote the expansion of opportunities for personnel to apply themselves diligently to acquire world-class competitive ability and the development of their capability to examine measures through research on such subjects as response methods, including attack methods and defense methods against cyberattacks, and the systematization of methods for collecting, analyzing, and evaluating information.

(3) Preparing a Foundation for Development of Cybersecurity Human Resource

In preparation for the evolution of information and communication technologies in the mid- and long-term, it is necessary to promote the understanding of the basic principles that form the foundation for cybersecurity as an applied sector and improve the initiatives for developing the ability to think logically and conceptually. To that end, regarding the fundamentals of cybersecurity and information and communication technologies, the industry, academia, and the public sector will collaborate to consider the knowledge and technology systems and a model curriculum based on those systems.

The government will also steadily work on fostering the ability to utilize information within the educational curriculum at the elementary and secondary educational level in order to strengthen the education among youth concerning cybersecurity and information and communication technology skills, including such measures as making computer science a required subject from elementary school, and cultivating logical modes of thinking, such as programmatical thinking, and an understanding of the systems and principles of information and communication technologies according to the levels of children's development. The government will place an emphasis on expanding and enrichment of training for teachers, while also working to ensure that course items regarding the fostering of the ability to utilize information are properly included in the teacher training courses. When doing so, it is important to promote the flexible utilization of personnel from industry as necessary. In addition, promoting information moral education is another important issue, due to the rise in cybercrime perpetrated by the youth in recent years.

Furthermore, it is also necessary to prepare an environment in which there are abundant opportunities for the youth, who are expected to acquire advanced cybersecurity skills in the future, to take an interest and learn freely using cybersecurity tools and devices in places outside

the school curriculum such as the community, companies, and organizations through the flexible use of industry personnel. At the same, it is considered that the development of this environment for self realization will be effective in preventing cybercrime perpetrated by youth out of curiosity when combined with ethics education. The government will also continue to promote the development of human resources for information technology in higher education such as universities and National institute of technology through industry-academia-public partnerships.

(4) Strengthening the Assurance and Development of Cybersecurity Human Resource at Agencies

The government will continue to work to steadily ensure and develop cybersecurity human resource at the Agencies under the command and control function of the full-time Assistant Vice Minister for Cybersecurity and Information Technology Management who carries out security measures based on the unified policy for governmental bodies. The government will also steadily carry out initiatives based on the human resource assurance and development plans of Agencies, through the increase of staff, training appropriate to each level for increasing knowledge and ability, and practice involving high level security technicians, and ensuring appropriate compensation, while working to further improve those initiatives through annual reviews of plans.

(5) Promoting International Partnership

Considering that the response to cybersecurity issues are needed on a global scale, Japan should enable the possibility for global application as much as possible as a part of the development of cybersecurity human resource, instead of fulfilling that need within Japan alone. To this end, the government will collaborate with leading nations to build a system for promoting collaboration in various ways with organizations engaged in human resource development overseas, such as the implementation of joint training programs and certification of credit transfer, by certifying the human resource development programs of universities and public institutions as meeting certain requirements according to international standards.

In addition, with the aim to contribute to the development of cybersecurity human resource overseas as well, the government will utilize the knowledge and experience gained through the development of cybersecurity human resource in Japan to contribute to the capacity building among cybersecurity human resource overseas.

4.4.2 Advancement of Research and Development

As the unification of cyberspace and real space continues, practical research and development (R&D) on cybersecurity is needed, given the advancement of innovation in cyberspace and the threat of cyberattacks against those innovations. Along with this, responses with a view to discontinuous evolution of technology and society over the mid- and long-term are also necessary.

(1) Promoting Practical R&D

Innovative new products and services are expected to be created through the combination of various information and communication technologies such as IoT and AI. The provision of products and services with a high level of security quality is essential when aiming for the growth of industry and the enhanced international competitiveness for Japan.

Meanwhile the use of these technologies has the potential to generate new vulnerabilities that did not previously exist. To that end, the government will work with a focus on technology that ensures cybersecurity through the use of such advanced technologies as AI and blockchain, security technology that can be built in to the systems comprising products and services, and practical R&D regarding the methods for such built-in security technology. In particular, the government will promote R&D on certification and generating trust, and ensuring traceability in the value creation processes of supply chains, and on detection of and defense against attacks in these areas. In addition, it will also engage in the development of technology to effectively detect malicious hardware and software built into devices and in R&D to ensure the authenticity, availability, and confidentiality of data and information when behavior unintended by the user may be caused on the platform.

The government will also promote R&D that increases situational awareness capabilities in cyberspace including the ability to detect and analyze cyberattacks, and contributes to ensuring national security in cyberspace, such as the improvement of defensive and response capabilities and ensuring of resilience. Specifically, the government will promote R&D with the aims to understanding attack activity by luring attackers into networks that imitate organization such as governmental bodies and companies, and to reduce the burden of wide area network scanning for the survey on vulnerable IoT devices on the network. In implementing this R&D, it is important to form a virtuous cycle in which the knowledge and experience of cyberattacks from the cybersecurity operations workplace is shared with researchers as quickly as possible for application in R&D, while the results of the R&D is also shared for application in the cybersecurity operations workplace as quickly as possible. To achieve this, the government will

promote the sharing of information in real time between security operations companies and governmental research and development institutions.

It is also important to ensure means to verify, as necessary, that malicious programs and circuits are not built into the devices and software used in the systems of governmental bodies and critical infrastructure operators. Accordingly, the government will take a central role to develop a system for carrying out the necessary technical inspections while also working on R&D necessary for that purpose. R&D will also be promoted on fundamental technologies that are essential to the state from the standpoint of national security, such as encryption technology that takes into account the development of computing technologies (e.g. quantum computing and AI).

Furthermore, in addition to these technology related R&D, research and studies on policy issues in cybersecurity measures will also be promoted, such as clarifying the interpretation of cybersecurity related laws and regulations.

Regarding these R&D initiatives for cybersecurity, the government will promote the dissemination and social adoption of the results. In addition, it will work to strengthen R&D-related international partnerships in the public and private sectors with like-minded countries that share basic values with Japan through joint research and the creation of international standards based on the research results while proactively participating in overseas events to disseminate information internationally.

(2) Responses with a View to the Mid- and Long-Term Evolution of Technology and Society

As the unification of cyberspace and real space proceeds, advancements in information and communication technologies such as AI and VR are making it possible to share diverse experiences including the processes by which they are formed, while acknowledging the different values of each individual. Amid the major changes to humanity brought about by these technologies, there is a possibility that the current received logic of social systems will fundamentally change in the future, and there will be a limit to what can be done with the existing approach of cybersecurity R&D that extrapolates from the evolution of technology so far. In order to generate new value, it is likely that a new approach will become necessary that designs overall society from the standpoint of the ecosystem, which humans are part of, looking ahead the future from the present where the continued unification of cyberspace and real space is taking place. To that end, with a view to mid- and long-term, the government will promote research on coordination and unification between cybersecurity various academic disciplines, including social scientific perspectives from the disciplines such as law and international relations, national

security, and business administration, and also the humanistic and sociological perspectives from the disciplines including philosophy and psychology. It goes without saying that the results of R&D, including R&D in the fields of science and technology, must not impact human society in a negative way.

4.4.3 Cooperation by Everyone who is the Main Player in Cybersecurity

With the spread of devices such as smartphones and public wireless networks, every people are connected to cyberspace and enjoys the significant benefits thereof. This trend is expected to accelerate with the advancement of IoT. Meanwhile, for the safe and secure use of cyberspace on a continuous basis amid the spreading threat of cyberattacks, it is essential for each and every people as an active agent in cyberspace to cultivate their awareness and understanding of cybersecurity so that they can deal with various risks in cyberspace in the same manner as the measures for crime prevention and traffic safety in real space, so that they can use cyberspace safely and securely.

For cultivating this awareness and understanding of cybersecurity, there is a limit to the effectiveness of existing campaign initiatives carried out by the state alone. Rather, 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 exercise its leadership through the approach to support such system.

Accordingly, with the National center of Incident readiness and Strategy for Cybersecurity playing the key role, the government will enable stakeholders in industry, academia, and the public and private sectors to operate smoothly and effectively and collaborate organically. Specifically, it will develop a comprehensive strategy and specific action plan for public awareness on cybersecurity and disseminate necessary information and handle inquiries by the people. The government will also promote practical action by the stakeholders by utilizing committees in which representatives of various communities in industry, academia, and the public and private sectors participate. The government will also work to further enhance Cybersecurity Awareness Month as a period to concentrate on promoting the understanding of cybersecurity by each and every people. It will also promote cybersecurity education through the creation and distribution of easy-to-understand guidebooks for people and through the development of the ability to utilize information through school curriculums.

Manufacturers and sellers of devices such as smartphones and personal computers and

telecommunications companies such as communications carriers and Internet providers are expected to enable users to carry out cybersecurity initiatives appropriately by providing security-friendly products and services and by explaining to users and responding to their inquiries. For this reason, the government will develop an environment that promotes initiatives by these businesses and related organizations and promote the development and steady implementation of guidelines useful to the establishment of cybersecurity based on user needs and usage forms.

5. Promotion and Implementation of Cybersecurity

The Government has been promoting a policy of improving cybersecurity measures to secure the use and application of information and communication technologies and data[61] as the socio-economic foundation of society[62] and to ensure Japan's national security.[63]

Under this policy, relevant governmental bodies should play their active roles in promoting cybersecurity measures, while making them consistent as a whole. For this purpose, the related government bodies will keep working on improving their cybersecurity capabilities under the leadership of the National center of Incident readiness and Strategy for Cybersecurity to ensure steady implementation of the measures stipulated in this strategy. The National center of Incident readiness and Strategy for Cybersecurity will play its leading role as the focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and the public and private sectors while disseminating this strategy to relevant parties in Japan and abroad. The Government will further reinforce its crisis management and response capabilities. In connection with the upcoming Tokyo 2020 Games, particular consideration should be given to steady implementation of cybersecurity measures by building up schemes of involvement, partnership, and collaboration of the industrial, academic, government, and community sectors.

The Cybersecurity Strategic Headquarters will closely work with the Strategic Headquarters for the promotion of an Advanced Information and Telecommunications Network Society when it works on critical cybersecurity issues. The headquarters will collaborate and share information with the crisis management organs, including a headquarters for emergency response to terrorism, when established, and take appropriate actions concerning national security, in close coordination with the National Security Council.

Furthermore, the headquarters will respond to issues concerning national security in close coordination with the NSC. In such cases, the relevant governmental bodies will work together under the overall coordination by the National Security Secretariat.

---

61 The Declaration to be the World's Most Advanced IT Nation: Basic Plan for the Advancement of Public and Private Sector Data Utilization (May 30, 2017) specifies that "In promoting the use and application of data, it goes without saying that measures should be concurrently carried out in connection with the protection of personal information and privacy, cyber-security measures, intellectual property rights, data quality and efforts to ensure the reliability and security of data, the state of logic in the era of AI and robots, and more".

62 Growth Strategy 2017 (Cabinet decision on June 9, 2017) states that "In the super smart society where people can live comfortably and abundantly in all situations, securing a safe cyber space is an important foundation for economic and social activities in Society 5.0."

63 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."

The Cybersecurity Strategic Headquarters will establish a budget prioritization policy and seek to secure and execute the budget necessary for the government so that the measures of the respective Agencies are steadily and effectively executed in accordance with the principles stipulated in this strategy. The headquarters will also encourage the collaboration between the public and private sectors to pursue effective intelligence and analysis capabilities, as well as mechanisms for flawless cycle of early detection, analysis, judgment and handling of cyberattacks.

Going forward, in order to implement this strategy in an accurate manner, the Cybersecurity Strategic Headquarters will set forth annual plans including the attached list of Agencies in charge during the three-year implementation period of this strategy, and the Agencies will steadily implement the measures on its basis. The headquarters will also review the status of progress of these measures, compile this as an annual report, and reflect it in the annual plan for the following year. Furthermore, since the situations and technical premises regarding cyberspace may evolve in a discontinuous manner, the strategy itself may be flexibly reviewed when necessary irregardless of the scheduled duration of the plan.