CYBERSECURITY POLICY COUNCIL REPORT

Cybersecurity Policy Council

December 17, 2021

Remarks on the Report

The advancement of digitalization in society has been causing cyberspace to transform into public space, following which concerns have arisen with the expanded damage and broader impact in the case of a cyber incident. Under such circumstances, it is necessary to undertake a sort of “all-Japan” measures, and the police are expected to play a central role in doing so.

Given these circumstances, in FY2022, the National Police Agency (NPA) will establish the Cyber Bureau within the National Police Agency, and also the National Cyber Unit, which undertakes investigations, etc., of grave cyber incidents, within the Kanto Regional Police Bureau. This will enable the centralization of investigating and unraveling situations of and taking countermeasures against cyber incidents. The NPA is also determined to adequately address cyber incidents that extend beyond national borders by building a relationship of trust with other countries’ investigative agencies and participating in international joint operations.

Such a large-scale reorganization, including reforms of bureaus, is to be made for the first time since the establishment of the Community Safety Bureau in 1994, and the NPA has been working on the reorganization, positioning it an issue of the highest priority. To establish the new organizations as truly effective ones, it was necessary to consider principles to be applied and specific initiatives after identifying emerging risks, etc., in a comprehensive manner.

Under the theme of the “policy package to be worked on by the new organizations including the Cyber Affairs Bureau,” the 2021 Cybersecurity Policy Council has been engaged in repeated discussions since September 2021 from a broad perspective and summarized them in a report.

Every one of us in cyber departments within the police is determined to do our best, keeping in mind what the report pointed out, that is, the Cyber Affairs Bureau and the National Cyber Unit should bear the heavy responsibility of playing a central role in protecting people's safe and secure lives in the new society where physical space and cyberspace as a public space are integrated.

In addition, while some risks emerging in digital society need to be addressed by the government or society as a whole, we will take the initiative and squarely work on measures that the police can undertake.

Full-fledged initiatives by cyber departments within the police are finally to begin with the establishment of the new organizations, and we are committed to cooperation with diverse stakeholders so that the advised principles will be shared among not only cyber departments but also the police as a whole and even stakeholders in the government, industry, and academia, and the specific initiatives result in the further development of "Japan as the Safest Country in the World."

河原 淳平

Jumpei Kawahara

Deputy Director-General for Cybersecurity and Informatization National Police Agency, Japan

[Summary for English translation]

This Report summarizes the results of discussions at the Cybersecurity Policy Council, consisting of experts with diverse backgrounds such as the industrial, academic, and legal communities, on such matters as the circumstances surrounding and roles to be played by the Cyber Affairs Bureau and the National Cyber Unit, which the National Police Agency plans to establish in 2022.

Following the advancement of digitalization, cyberspace will become increasingly positioned as an important public space where all the people participate to engage in social and economic activities autonomously.

Meanwhile, the threats in cyberspace remained grave, as exemplified by a significant increase in damage caused by ransomware to companies, organizations, and other institutions in Japan, and many cyberattacks against Japanese government agencies, research institutions, and other entities. Moreover, against the backdrop of the integration of cyberspace and real space following the advancement of digitalization, the degree of threats of crimes straddling both spaces is heightening, as seen in the increase in damage caused by kidnapping in relation to social networking services (SNS).

To address these serious threats, the National Police Agency will establish the Cyber Affairs Bureau as its internal department, which will centrally take charge of policies related to cyber incidents, and also the National Cyber Unit, which will undertake investigations and international joint operations against serious cyber incidents (incidents behind which exists a state, etc.), in 2022.

These new organizations must face up to not only risks that have already come to the fore but also risks that are emerging, such as the difficulty in foreseeing the scope of impact of a cyber incident or unraveling and taking countermeasures against incidents due to increasingly complex supply chains, and continue to protect the people’s safety into the future.

To do this, the new organizations must play a central role in ensuring the safety and security of a digital society where physical space and cyberspace are integrated, in cooperation with existing police departments and diverse stakeholders alike.

Issues to be solved to fulfill the role are sorted out and classified broadly into four categories, namely, “Strengthening of the handling system” to promote measures properly; “Strengthening of international collaboration and response” to push forward with effective initiatives against the cross-border nature of cyberspace; “Strengthening of the abilities to ascertain situations and adapt to social change” to respond to an ever-changing society where new technologies and services are created on a daily basis; and “Safety and security generated by society as a whole” to push forward with initiatives based on a multi-stakeholder process, and measures that should be undertaken to solve each of the issues are presented.

Contents

Introduction

The 2020 Cybersecurity Policy Council advised that it was necessary to place "ensuring safety as a public space" as a new fundamental principle for future cybersecurity, amid circumstances where cyberspace continues to transform, following the advancement of digitalization, into a public space where all the people are involved. This principle has become established as a socially shared recognition, as exemplified by the fact that the national government's new Cybersecurity Strategy states that it is necessary to "cyberspace must have the same level of safety and security as real space in order to be recognized as a public space."

Meanwhile, the threats in cyberspace remained grave, as exemplified by not only a significant increase in damage caused by ransomware to companies, organizations, and other institutions in Japan but also many cyberattacks against Japanese government agencies, research institutions, and other entities. Moreover, against the backdrop of the integration of cyberspace and real space following the advancement of digitalization, the degree of threats of crimes straddling both spaces is heightening, as seen in the increase in damage caused by kidnapping in relation to social networking services (SNS).

To address these serious threats, it is necessary to build an effective handling system by centralizing resources within the National Police Agency, which until now have been decentralized; to ascertain the complete picture of incidents accurately, and coordinate investigations and countermeasures for them; and, further, promote international investigations in collaboration with overseas public security authorities, etc. The following characteristics are notable in investigations of recent grave cyber incidents in particular.

- National nature: In international joint operations with overseas public security authorities, etc. and investigations aiming to unravel the responsibility of a specific country, the investigative entity represents the national government, and the national government itself may be required to be the investigative entity depending on incidents.
- Non-regional nature: Only a shallow geographic connection exists between where attackers are located and where damage occurs, and damage easily spreads. In addition, regions requiring investigations are also scattered.
- Necessity of consolidating resources for handling: A high level of technological prowess and building of readiness are required to unravel incidents, but it is difficult or inefficient to take action if resources are scattered across Japan; thus these resources need to be consolidated.

Accordingly, based on the recognition of these circumstances, in FY2022, the National Police Agency will establish the Cyber Affairs Bureau as its internal department, which will centrally take charge of policies related to cyber incidents, and also the National Cyber Unit within the Kanto

Regional Police Bureau, which will serve as an investigative unit of the national government. The Cyber Affairs Bureau is expected to play a role in such matters as the central consolidation and analysis of various types of cyber information, implementation of effective countermeasures and collaborations related to cyber incidents, and close collaborations with overseas public security authorities, etc., while the National Cyber Unit is expected to play a role in supplementing investigations currently undertaken by the Prefectural Police departments alone and undertaking international joint operations and investigating serious cyber incidents itself as an organ of the national government, based on the above-mentioned national nature, non-regional nature, and necessity of consolidating resources for handling.

To establish the Cyber Affairs Bureau and the National Cyber Unit as truly effective organizations, it is necessary to include the consideration from a broad and panoramic perspective, such as the consideration of principles to be applied, as well as the detailed review of specific initiatives. To accomplish this, at first, risks that are emerging following the advancement of digitalization and the widespread use of new technology, among other things, need to be identified broadly. Moreover, to advance the consideration appropriately, it is indispensable that diverse stakeholders get involved not only from within police departments but also who have the specialization and consider things from a broad and panoramic perspective and the people’s point of view.

Accordingly, under the theme of the “policy package to be worked on by the new organizations including the Cyber Affairs Bureau,” the 2021 Cybersecurity Policy Council has been engaged in repeated discussions since September 2021 from a broad perspective.

This Report summarizes the results of discussions at this Council on circumstances surrounding cyberspace and its risks, roles expected of the Cyber Affairs Bureau and the National Cyber Unit, policy issues in fulfilling such roles, and specific measures to solve the issues.

1 Recognition of circumstances

1. 1 Cyberspace as it becomes increasingly public

(1) Cyberspace as it becomes increasingly public

Cyberspace has been seen as a “frontier for generating infinite value[1],” a place in which intellectual property, such as technological innovations and new business models, can be created, as well as a place where people can utilize creation and innovation to expand their activities significantly.

In fact, the use of cyberspace has broadly spread in people’s lives, as exemplified by the facts that the internet usage rate of individuals reached 83.4% in 2020 and the usage, including the use of SNS and voice call apps, information retrieval, and purchase of products and services, has become diverse[2]. In addition, digital services provided in cyberspace have advanced significantly through an increase in the amount of data, cyberspace can handle and the development of information and communications technologies, such as the internet of things (IoT) and artificial intelligence (AI).

Moreover, the establishment of a “new lifestyle” following the spread of COVID-19 and the associated advancement of digitalization in society further accelerated these situations. During this period, business operators in various industries and business categories that were hitherto unrelated to cyberspace started providing services using cyberspace. In addition, social activities assumed to be conducted face-to-face in real space have been transformed significantly to be conducted non-face-to-face and contactless through cyberspace. It is not an overstatement to say that, under such circumstances, cyberspace has become increasingly positioned as an important public space where all people, regardless of age or gender, participate and engage in social and economic activities.

In our daily lives, it has become common to check the news every morning using smartphones, eat foods purchased from e-commerce websites, do work or participate in classes online, communicate with friends through SNS, and spend our spare time watching online videos. Cyberspace fulfills functions and roles comparable to public facilities in real space, which are broadly open to and used by people as a place for social and economic activities, such as schools, parks, and libraries.

Indeed, cyberspace does not have a substance as a “space,” and its substance is rather an aggregate of physical equipment such as terminals, network devices, and storage devices. In addition, many of the devices are an assemblage of private property managed by private business

[1] Cybersecurity Strategy (approved by the Cabinet on July 27, 2018), page 1.

[2] WHITE PAPER 2021 Information and Communications in Japan, pages 50 and 55.

operators. However, the “place,” which is comprised of aggregates of various kinds of physical equipment, is conceived as a “place” available for everyone (public nature as a concept) through the use of devices, etc. Precisely because such recognition is shared, in reality, an enormous amount of information is exchanged daily, and economic activities frequently take place through this “place.” Nowadays, dependency on networks has been rapidly growing (public nature in real society) not only at an individual level but also in society as a whole. Given this situation, it is essential to recognize this “place” as a “cyberspace” and deepen the shared understanding of a high level of public nature and the key roles of cyberspace in modern society, which is nothing else but public space.

(2) Safety and security as public space

According to a questionnaire survey[3] concerning trends in crime conducted by the National Police Agency in 2020, about 75% of respondents said that they harbored a sense of anxiety about their involvement in cybercrime. This result is in stark contrast to the situation where “the high level of public security” ranked first for many years as the answer of what respondents were proud of Japan.[4]

It is also suggested that there are significant gaps in awareness and knowledge that individuals have concerning cybersecurity, as seen in the fact that, although people harbor such a sense of anxiety, specific measures may not always be sufficiently invoked at an individual level from the feeling of anxiety[5]. For example, the Public Opinion Poll on Safety and Security of the internet[6] conducted by the Cabinet Office revealed that at least 60% of respondents who had not taken measures to use the internet in a safe and secure manner said that they were “not sure what I should do.” Similarly, security measures by business operators vary depending on the size and industry of the business operators[5].

The fact that people broadly harbor a sense of anxiety about cyberspace and the situation in which significant differences in knowledge and initiatives concerning cybersecurity exist among individuals and business operators as described above have weakened the functions and roles of cyberspace as public space and thus posed serious issues directly linked to risks of which attackers would take advantage.

[3] Crime Situation in 2020 (Commissioner General’s Secretariat of the National Police Agency)

[4] Public Opinion Poll on Social Awareness (March 27, 2020, Cabinet Office), 2.2(3).

[5] Cybersecurity Awareness and Behavior Strengthening Program (approved by the Cybersecurity Strategic Headquarters on January 24, 2019), pages 4 through 6.

[6] Public Opinion Poll on Safety and Security of the internet (November 2, 2018, Cabinet Office)

It is indispensable for those involved in cyberspace to recognize their own roles in cybersecurity and undertake cybersecurity initiatives autonomously to increase society's resilience as a whole and deter the activities of malicious actors[7]. Based on the foregoing, cyberspace has become a place that fulfills functions and roles as a public space where everyone is involved, as well as a place where safety and a sense of security are expected. It might be necessary that each individual and business operator undertakes autonomous initiatives, public institutions such as the police play required roles, and thereby safety and security are ensured in cyberspace at the same level as physical space.

(3) Discussions at the 2020 Cybersecurity Policy Council

The 2020 Cybersecurity Policy Council had broad discussions under the theme of "Further promotion of public-private collaboration to address new cyberspace threats associated with a change in lifestyles."

In the discussions, matters such as:

○ that cyberspace will become increasingly positioned as an important public space where all the people, regardless of locations and ages, ranging from children to the elderly, participate and engage in social and economic activities; and

○ that, given that cyberspace has gotten to be required to fulfill its role as a public space, even if it is an assemblage of private property, it is necessary that cyberspace must have the same level of safety and security as real space in order to be recognized as a public space;

were confirmed, and the Council decided to advise that it was necessary to place "ensuring the safety as public space" as a new fundamental principle for future cybersecurity.

This principle has become established as a socially shared recognition as exemplified by the fact that the Cybersecurity Strategy (approved by the Cabinet on September 28, 2021) states on page 11 that "cyberspace must have the same level of safety and security as real space in order to be recognized as a public space. To this end, Japan must […][,] without overlooking the asymmetrical situation with attackers, […] work to improve the environment and address the causes."

1. 2 Integration of real space and cyberspace

(1) Accelerated digitalization

The advancement of digitalization in society continued to accelerate after the 2020 Cybersecurity Policy Council submitted its report.

[7] Based on the idea that cyberspace should be "a free, fair, and secure space," the Cybersecurity Strategy (approved by the Cabinet on September 28, 2021) upheld the "autonomy" (meaning that various social systems autonomously fulfill their roles and functions to maintain order in cyberspace) as one of the basic principles to be followed in formulating and implementing measures on cybersecurity.

The Digital Agency was established in September 2021 to lead the effort in creating a digital society and powerfully promote digital transformation under the vision of creating "a society where people can choose services that suit their needs and realize diverse forms of happiness through the use of digital technology,"[8] with the aim of achieving "people-friendly digitalization, with no one left behind." As exemplified above, the government has advanced the establishment of systems and is proactively pushing forward with related business.

[Case example]

○ *As of the end of July 2021, 96.2% of public elementary schools, etc. and 96.5% of junior high schools, etc., across Japan started using devices under the GIGA School Program*[9]*.*

○ *In October 2021, the Digital Agency held a public tender for leading projects related to the Government Cloud*[10] *and selected cloud service providers and eight municipalities for these.*

In addition, the private sector has also made significant advancements in digitalization, as exemplified by the facts that the ratio of companies that answered that they commenced initiatives related to digital transformation (DX) hiked significantly from 28.9% in 2020 to 45.3% in 2021[11], and cases were observed where initiatives went beyond the introduction of information technology (IT) in existing operations.

[Case example]

○ *In April 2021, a leading trading company announced that it had commenced a DX project for an overseas mine.*

The project plans to visualize operational data as well as management and financial data and implement preventive maintenance of related material and equipment in the first phase, and aims to improve efficiency through the integration of data covering everything from mine operation to port and harbor operation as well as linkage with head office functions and market information in the second phase and onward.

○ *In April 2021, an industry-academia-government group, including a national university, announced that it conducted a verification test related to remote control of robot-assisted*

[8] Basic Policy on Reform toward the Realization of a Digital Society (approved by the Cabinet on December 25, 2020), page 2.

[9] This program seeks to provide one computer for every student and broadband communication networks to schools to realize individually optimized and collaborative learning for all children to bring out their potentials. The numerical values are excerpted from "Survey on Device Usage (As of the End of July 2021) (Definite Value)" (October 2021, the Ministry of Education, Culture, Sports, Science and Technology), page 1.

[10] A shared cloud service usage environment for government entities. The Priority Policy Program for the Realization of a Digital Society (approved by the Cabinet on June 18, 2021) states in page 13 that "all local governments aim to move […] and conform to the standardization criteria by FY2025, the target timing.

[11] Japan Management Association "42nd 'Survey on Imminent Corporate Management Challenges' 2021"

surgery via commercial 5G networks. This initiative is positioned as a preliminary step toward remote robotic surgery.

In addition, various initiatives such as an experiment in which AI learns and practices sutures after surgical operation have been launched in the United States.

○ *In September 2021, the media reported that a leading convenience store operator planned to roll out about 1,000 unstaffed shops using AI and various sensors by the end of FY2024.*

(2) Phenomenon in which real space and cyberspace are integrated following the advancement of technology and infrastructure

The establishment and widespread use of technology and infrastructure have also been significantly advanced.

The personal smartphone ownership rate reached 69.3% in 2020. In addition, both displayed image and voice quality has improved as the computing and communications functions of devices, such as smartphones and personal computers, owned by individuals have significantly improved; also, interfaces for input and output functions and others have become increasingly diverse. Furthermore, applications and services that can be used on devices have been enhanced in terms of quality and quantity.

Personal information devices, including smartphones, now fulfill not only specific purposes such as communication but also the role of an "entrance to cyberspace." Smartphones, which can be taken along in people's lives at all times, provide users with an environment where they can access cyberspace at high speed anytime and anywhere. Moreover, interfaces that enable intuitive and interactive operation and high-quality images and audio may provide users with a realistic feeling and a heightened sense of immersion similar to real space thanks to further improvement of functions in the future.

It is also likely that real space and cyberspace for peoples' lives will function as a highly integrated place where they can go back and forth freely and conduct activities without consciously distinguishing a clear boundary, when cyberspace further provides convenient services highly linked with physical space and more diverse types of entertainment than physical space.

As an example in terms of communications infrastructure, communications environments have so far been built around places where people are, such as place of residence or work, for them to access cyberspace. In recent years, however, initiatives related to satellite constellations have been undertaken to enable high-speed, wide-bandwidth data transmission across the surface, regardless of whether by land, air, or sea, through the collaboration between a large number of small nongeostationary satellites deployed in medium and low Earth orbits. It would become possible to connect to cyberspace anytime and anywhere in the future. In addition, the penetration of the fifth-generation mobile communication system (5G) capable of ultra-high-speed, wide-bandwidth, low-latency, and massive concurrent connections may enable accurate control of remotely located devices or allow devices to collect and control related data autonomously through cyberspace, without needing human intervention.

As described above, in a society where anyone (or anything) is assumed to be able to connect to and conduct activities in cyberspace anytime and from anywhere in real space (i.e., a society where 100% coverage rate is assumed), the high degree of integration between physical and cyberspace may further advance, beyond geographic and/or time restrictions, in terms of everything from daily lives to state functions. Society 5.0, which can achieve both economic development and solution of social issues, is gradually becoming a reality.

[Case example]

○ *Base stations have been developed for 5G technology, which was commercialized in March 2020, and in January 2021, a leading communications carrier announced that it was slated to achieve 90% population coverage in March 2022.*

○ *In September 2021, a leading communications carrier announced that it would start introducing satellite constellations around 2022 in collaboration with U.S. companies. In addition, the priority matters toward the revision of the Implementation Plan of the Basic Plan on Space Policy decided in June 2021 (by the Strategic Headquarters for Space Development on June 29, 2021) included the promotion of strategic initiatives toward the establishment of Japan's own satellite constellations.*

○ *Also advancing are the further sophistication of the characteristics of 5G technology as well as research and development toward Beyond 5G in which different communications systems such as satellite constellations and the High Altitude Platform Station (HAPS) (which uses unmanned aircraft flying in the stratosphere as base stations) are seamlessly connected and which has the scalability to make communication available anywhere.*

Against this backdrop, in a society where real space and cyberspace are integrated, tremendous benefits are expected to be brought about to people in, for example, the following forms through a data-driven economy in which data, so-called "the new oil of the 21st century," creates new value.

○ Value such as craftsmanship, which is rooted within an individual or group and the broad use of which has been difficult because long-term training is required to succeed or reproduce it (tacit knowledge, etc.), will be made into data and made available for generalization and use, and, thereby, high-quality services will be broadly provided.

○ Diverse data will be fed back to the real space via IoT devices, etc., and thereby new products and services (preventive maintenance, automatic operation, formulation of business plans, etc.) will be created.

○ Quality of life will improve thanks to such events as the provision of flexible services customized for each individual based on registered information, etc. of individuals

1. 3 Emerging risks

1. 3. 1 Risks associated with digitalization

As described in 1.2(2), in a society where real space and cyberspace are integrated, it is expected that convenience in our lives will improve, and furthermore, value created through the use of an enormous amount of data distributed through cyberspace and various information and communications technology will be significantly increased.

Meanwhile, it is necessary to direct our attention to risks that might emerge. The increased value of data will undoubtedly expand damage in the event of theft or destruction of data to an unprecedented degree. In addition, the amount of information in cyberspace and the computing capability of devices may sooner or later exceed the cognitive and judgment abilities of human beings in every situation significantly, and misunderstanding or misjudgment of human beings involved in cyberspace may cause various situations where, for example, cleverly fraudulent acts are prevalent to happen. Furthermore, the evolution of mutual linkages among digital services and supply chains may make it more difficult to foresee the scope of impact of a potential cyber incident or unravel and take countermeasures against incidents. As described above, potential damage and the scope of impact therefrom in the event of cyber incidents have increased to an unprecedented degree compared with the past, causing vulnerabilities in which the safety and security of people's lives are exposed to significant risks.

While it is extremely challenging to exhaustively sort out risks that might emerge in close association with these benefits of digitalization, some representative examples of risks are presented below from the three perspectives: an increase in value of data and expanded potential damage; limitations in cognitive and judgment abilities of human beings; and the expanded scope of impact of cyber incidents.

(1) An increase in value of data and expanded potential damage in cyberspace

(i) Theft of "new value" through data theft

Data accumulated in cyberspace has been steadily increasing in terms of both quality and quantity following the advances in communications technology and IoT technology. In addition, the value of existing data also tends to rise as methods of processing and using data have become more sophisticated due to the development of AI. Such a rise in data value means a concurrent increase in the value lost in the event of theft of such data.

Previously, information targeted for theft through cyberattacks was cutting-edge technological information and/or customer information held by companies. This was due to restrictions inherent in the acts of theft that subjects of the theft are limited to information stored as electromagnetic records capable of being copied or transmitted.

However, as mentioned above, if value such as craftsmanship which exists within an individual or group and the visualization (putting into words) of which has previously been difficult can also be made into data, the value itself may be stolen and reproduced.

For example, it is said that Japan’s manufacturing process technology is one of the country’s strengths and represents the accumulation of the experience and expertise of engineers based on close collaboration and coordination throughout the value chain[12]. However, if such value as a strength of the Japanese economy is stolen, it might pose a threat that could disrupt Japan’s social infrastructure as a whole from the perspective of economic security.

In addition to data theft, it can also be a threat if data that has already been broadly leaked or disclosed, or which has been obtained by conducting advanced analysis or processing of the foregoing data using information and communications technology such as AI, is exploited.

For example, while online identification of people is broadly conducted across the world using electronic Know Your Customer (eKYC) authentication with data such as face images and videos showing how people look, it is pointed out that there is a risk even now that data such as face images and videos for authentication use which seems to have been stolen is already distributed in the dark web, etc. and attackers use this to pass authentication illegally. There is also a future risk that attackers break through various authentication systems, including verification with images, using biometric authentication data which is “created (processed by combining data that has been leaked, etc.)” using technology such as deepfakes, instead of such data considered to have been stolen from the data subject, and conduct such activities as illegally opening accounts.

In addition, cases have already been confirmed in which graduate directories of junior high schools, senior high schools, etc. were exploited for selecting phone call targets by billing fraud groups, but it is expected that similar exploitation of information would occur in

[12] Materials Innovation Strategy (approved by the Council for Integrated Innovation Strategy on April 27, 2021), page 16.

cyberspace as well. For example, there is a possibility that risks such as the following broadly arise in the future: Attackers collect and analyze data in cyberspace, such as SNS posts, presume and ascertain information of an attack target, such as which elementary school the target went or the name of their pet, which should have been known only by the target, and illegally pass knowledge-based authentication (authentication of a user using information that only the user knows, such as the ID and password and the answer to a security question).

As described above, attention needs to be paid also to the fact that new risks may arise due to advanced analysis and processing of data that has already been broadly leaked or disclosed, using information and communications technology such as AI, and to risks such as exploitation of the foregoing data for new purposes in digital services, etc. among which mutual linkages are evolving.

(ii) Expansion of damage caused by data poisoning

Damage has been relatively limited in scope in terms of damage caused by data poisoned due to reasons such as the inclusion of illegal data through cache poisoning, where visitors are guided to unintended websites because cache information in domain name system (DNS) servers[13] has been altered or through chatbots reacting inappropriately because they have acquired malicious data.

However, data reliability is a life or death matter in social and economic activities in a situation where control of various devices and corporate activities are dependent on data. For example, a serious accident involving human lives may occur due to a malfunction in controlling devices supporting lifelines, autonomous vehicles, remote surgery robots, etc. If input data has been replaced with illegal data, and economic damage that may endanger a company’s existence may occur to the business operator if business planning and operational decisions have been disrupted due to data poisoning.

In addition, a technique called backdoor attack may be used against AI, in which the AI will falsely recognize specific input data as data input by an attacker due to illegal data included in training data. There is a possibility that cases such as the following occur if such technique is used: a person who has not been appropriately authorized can pass the authentication and enter or exit a room or building when an image recognition camera is used for entry/exit authentication; and a remote surgery device may cause harm due to a malfunction, a trigger for which is set as the recognition of that specific person.

[13] Applications and server devices that provide name resolution (translating domain names and host names to IP addresses) services.

As described above, threats of data poisoning by attackers could rise to the extent of affecting human lives and the existence of companies.

(2) Exploitation of limitations in cognitive and judgment abilities of human beings

(i) Expansion of damage caused by strengthened defrauding ability

Even now, criminal techniques exploiting a cognitive error or misjudgment of others, such as cheating people out of their money by pretending to be someone, are causing much damage.

The number of phishing cases, many of which have caused damage from remittance fraud of internet banking, reported to the Council of Anti-Phishing Japan in 2020 was 224,676 (an increase of 168,889, or 303%, year on year)[14], a significant increase from the previous year.

In addition, damage from special fraud cases[15] in real space has also been occurring at a high frequency, mainly in the elderly. The total amount of damage from “it’s me/ore-ore” fraud and savings fraud (which has been included in “it’s me/ore-ore” fraud up to the previous year) in particular in 2020 was 12.61 billion yen (an increase of 0.85 billion yen, or 7.2%, year on year), an increase from the previous year.

Furthermore, a technique linking cyberspace and real space has been observed, such as technical support fraud, in which a website displayed by using a search engine online skillfully guides the visitor to make a phone call to involve them in a crime.

The advancement of digitalization gives an opportunity also for criminals to exploit an enormous amount of data such as preferences, movement history, etc. of individuals distributed in cyberspace and information and communications technology. For example, concerning the existing threats mentioned above, it is possible to reproduce an actual person with a high degree of accuracy in cyberspace by exploiting machine learning, etc. in combination with an enormous amount of information in cyberspace, which in turn makes it possible to conduct phishing fraud, special fraud, business email compromise, spear phishing attack, etc. using details based on attributes and backgrounds of individual targets. In addition, it may also be possible that threats of fraud such as special fraud (where the use of not only phone calls, which account for most current means of fraud, but also video calls and other similar means would become possible) may explosively increase if a high level of fraudulent means can automatically be mass-produced both visually and aurally by combining more

[14] Aggregated based on monthly reports issued by the Council of Anti-Phishing Japan. (https://www.antiphishing.jp/report/monthly/)

[15] A collective term referring to crimes of cheating many and unspecified people out of cash, etc. by using methods such as calling victims on the phone, making them fall for fast talking without seeing them face to face, then transferring their cash to a designated savings account or otherwise (including extortion for cash, etc. and cash card fraud or theft).

sophisticated details with technologies such as deepfakes, which generate videos and voices imitating real persons using machine learning.

As described above, we need to recognize also new threats where technology is exploited and causes the existing threats of cheating people out of their money through fraudulent means to increase and spread to an unprecedented degree in terms of both quality and quantity.

(ii) Occurrence of infodemic

Following the development of SNS, etc., it has become a social issue to cope with infodemic (a term created by combining information and epidemic, meaning a phenomenon in which a large amount of information, whether accurate or inaccurate, spreads like an infectious disease and exerts an impact on real society), or to address the distribution of false information or the overflowing of biased information in particular.

[Case example]

○ *A survey conducted by the Ministry of Internal Affairs and Communications*[16] *revealed that there was a considerable number of people who believed wrong or misleading information or who could not determine whether such information was accurate or not, as seen in the fact that, with respect to false information related to COVID-19 (such as "drinking water frequently is effective for preventing COVID-19"), about 30% to 60% of respondents answered that they "thought the information was not correct/did not believe the information," except for certain information.*

○ *Regarding the incident of toilet paper having been bought up across Japan in 2020, a report said that this was caused by the explosive spread of postings denying a false rumor about toilet paper expected to be out of stock, instead of postings of the false rumor themselves.*

Such distribution of false information is not a problem unique to the internet. There have been past cases where less trustworthy information that may or may not be true was spread by word of mouth and other ways. However, it is believed that such a significant problem as the infodemic has emerged due partly to the nature of SNS, etc. have concerning the flow of information, which are, e.g., information being spread more easily, "echo chambers[17]" in which specific opinions are amplified and become more influential through interactions and

[16] Survey Report on COVID-19 Information Distribution (Ministry of Internal Affairs and Communications), page 18.

[17] According to the WHITE PAPER 2019 Information and Communications in Japan, page 102, "The term is an analogy of a physical phenomenon in which a sound resonates in a closed small room used to refer to a situation in which a user of social media follows other users who have similar interests and concerns to their own, which results in receiving opinions similar to their own in response to their opinions shared through SNS."

sympathies among people with similar values, and "filter bubbles[18]" in which users are isolated from society in terms of ideas due to the selective presentation of information that is favorably received by the users themselves. In addition, it is reportedly often the case that confusion is aggravated in a manner unintended by parties sending out information. Meanwhile, due attention should also be paid to the possibility of acts that intend to exploit such characteristics and cause social disorders, such as making illegal gains of any sort and manipulating public opinion through the broad and intentional distribution of false information or biased information.

(3) Expanded scope of impact of cyber incidents

(i) Expansion of damage due to supply chains becoming more complex and obscure

As supply chains have become more complex and digital services more connected, it has inherent risks that the scope of impact would significantly expand once a cyber incident occurs.

For example, the widespread use of IoT devices in people's lives and industries indeed has been leading to the advent of a society where everything is connected to the internet, which at the same time means that cyberattacks would have a direct impact on people's lives and industries in every situation. If owners, etc. of widely spread IoT devices do not take sufficient security measures but leave vulnerabilities untreated, an enormous number of IoT devices may be hacked and exploited for distributed denial of service (DDoS) attacks. As such, it is necessary to understand risk factors from even more diverse perspectives. In addition, an impact on people's lives would naturally be profound, if cyberattacks on controlling systems owned by business operators of critical infrastructure hinder the provision of important infrastructure services.

In fact, as supply chains have become more complex and digital services more connected, situations have been observed in which the impact of a failure of or a cyberattack against infrastructure for communications, etc.

[Case example]

○ *In a large-scale communication failure that occurred in October 2021 at a leading communications carrier, the number of its users who were unable to talk on the phone or use data communications reached about 1 million and it became difficult to use part*

[18] According to the WHITE PAPER 2019 Information and Communications in Japan, page 103, "An information environment in which individual internet users are isolated in a 'bubble' of their own thoughts and values, separated from information which disagrees with the users' viewpoints, as algorithms analyze and learn search history and past click-behavior of them and selectively display information that the users would want to see, whether the users so intended or not."

of cashless payment services dependent on the carrier's data communications services. In such and other ways, the failure caused a broad impact on people's lives.

○ *In December 2020, a leading U.S. IT infrastructure management software company suffered a cyberattack; as a result, illegal code was embedded in update files related to its products, and vulnerabilities spread across its customers who updated the products, causing an impact to organizations around the world, including a large number of U.S. government agencies.*

○ *It was reportedly highly likely that the cyberattacks against about 200 companies, etc. in Japan, including the Japan Aerospace Exploration Agency (JAXA), during a period from 2016 to 2017, were carried out after the attackers obtained IT asset management software, which was sold only in Japan, and examined its vulnerabilities in advance.*

In addition, in illicit transfers via cashless payment services that occurred during 2020, vulnerabilities in identity verification methods used at the time of unconsented linking to the victims' banking account were exploited.

Furthermore, credit card information is now linked to various services following the widespread use of cashless payment services. Many incidents of unauthorized use of credit cards have occurred, whether in cyberspace or real space, and the amount of damage is also increasing, for example, from 13.22 billion yen in the second half of 2020 to 15.56 billion yen in the first half of 2021[19].

As described above, given how services are linked in a complicated manner, there is a possibility that unexpected damage occurs, as the full picture of how identity is verified across the linked services and what security measures are taken becomes unclear.

It is expected that, in the future, the scope of impact of accidents, cyberattacks, etc. expands considerably, and it becomes difficult to ascertain where the impact occurs, due to the widespread use of new technologies and the complexity of supply chains, etc. becoming more digitized.

In addition to cases related to mines as described in 1.2(1), digitalization in the primary and secondary industries has been advancing. For example, data is used in agriculture when determining the timing of spraying agricultural chemicals and harvesting. Examples of risks include that cyberattacks are carried out against such suppliers of raw materials, etc. to cause them to suspend their operation, and attacks are carried out to obtain illegal gains in the

[19] "Status of Occurrence of Damage From Unauthorized Use of Credit Cards" (Japan Consumer Credit Association, September 2021)

commodity futures market, etc. by ascertaining the amount of supply in advance based on stolen data. In addition, given how various services deepen their linkages in identity verification, authentication, and various other phases, such as substituting identity verification at the time of opening cashless payment services accounts with identity verification by banks, etc. that are linked with banking accounts, damage may occur to existing important services which have robust security themselves, if security is vulnerable or identity verification procedures are lax at separate services on the route to them.

(ii) Expansion of damage to children and young people

As many people are now involved in cyberspace, damage to children and young people occurred through cyberspace also has been expanding.

[Case example]

○ *The number of cases of bullying where bullied ones were "slandered, libeled, or harassed using personal computers, mobile phones, etc.," among modes of bullying recognized, was 18,870, combining answers from elementary schools, junior high schools, and senior high schools, hitting a record high*[20].

○ *The number of children under 18 years old who fell victim to kidnapping by enticement or force in relation to SNS was 75 (up 63% year on year), and the entire number of victimized children combining those under the Child Welfare Act, Prefectural Ordinances of Juvenile Protection, the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children grave crimes, etc. was 1,819, remaining at a high level*[21].

Among the victimized children above, 984 out of 1,151 who provided an answer said that they did not use filtering, accounting for about 85%.

○ *Amid the situation where devices are broadly provided under the GIGA School Program, 39.3% of junior high school respondents answered that they had encountered troubles (communication troubles, browsing of inappropriate websites, matters related to personal information and privacy, etc.) through the internet while children and students were using devices for learning*[22].

[20] Results of the FY2020 Survey on Problems of Pupil Guidance for Behavior Problems of Students (Ministry of Education, Culture, Sports, Science and Technology, October 13, 2021), pages 3 and 31.

[21] Status of Delinquent Acts, Abuse and Sexual Abuse of Children in 2020 (National Police Agency, March 2021), page 20.

[22] Survey Report on the Use of ICT in the One-Device-Per-Student Environment and the Practice of Information Moral Education (Line Mirai Foundation, August 2021), pages 20 and 22.

In real space, multi-faceted and multi-layered frameworks to ensure the sound development of children and young people exist in such ways as that acts and environments that may hinder the sound development of juveniles are regulated by ordinances, etc., entry of the youth to certain facilities is restricted, and the sale of harmful books, etc. to young people is prohibited. In contrast, in cyberspace, situations are observed in which, for example, the use of SNS apps is left to the discretion of parents or guardians, etc. The future issue is the sound development of the youth in digital society in which participation by children and young people will be further accelerated.

(iii) Expansion of damage caused by advancement of cross reality technologies

The metaverse (a coined word generated from "meta" and "universe," meaning a three-dimensional virtual world built in cyberspace and participated by a large number of people) may rapidly become common in the future following the advancement of cross-reality technologies such as virtual reality (VR) and augmented reality (AR).

[Case example]

○ *A leading communications carrier announced in September 2021 that it was planning to build a virtual urban infrastructure in virtual reality where various activities can be conducted and start provision thereof in 2022.*

○ *A U.S. leading SNS provider announced in October 2021 that it would focus on the metaverse in line with its plan to change its corporate name.*

○ *A U.S. leading software developer announced in November 2021 that it would start providing tools to enable such work as participation in online meetings and joint operations in virtual reality in 2022.*

The metaverse is considered to be a space for free activities and interchange with others for avatars (graphical representation of users in virtual reality), and also a place to sell and buy or consume services and contents in various fields, rather than a place for activities conducted in a confined space and under certain restrictions as with the case of previous online games participated by a large number of people.

As the metaverse becomes common, various risks that have already emerged or are currently emerging are expected to increase or be more serious. For example, unlike imitation of real persons, etc. such as deepfakes, it is easy to reproduce the appearance of avatars, which are originally nothing more than electronic data, and it is expected that identity verification, etc. becomes even more complicated, damage from spoofing and other attacks expands, and the traceability after incidents is hindered.

In addition, it is also expected that cyberspace will play a more important role than real space in the future, in such a way as that an economic zone greater than that of real space will be formed through the use of services, and the flow of "currencies" within the metaverse, going far beyond the current situation where key activities such as transactions and meetings that used to be conducted in real space, are coming into cyberspace. In such a new form of society, a series of risks can also emerge in addition to new benefits that cannot presently be anticipated.

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

Cyberspace has been part of a realm of interstate competition that reflects geopolitical tensions, where it seems that threats of cyberattacks have been increasing in recent years[23].

Cyberattacks in which state involvement is suspected include those conducted to steal information from government agencies, companies with cutting-edge technologies, etc., exert influence to achieve military or political aims, and obtain foreign currency[23].

Amid the situation where threats have been increasing as described above, the situation in cyberspace can no longer be deemed purely peacetime or wartime[23].

Moreover, in addition to direct cyberattacks, differences in basic value have become apparent and conflicts have arisen over international rules and other matters concerning cyberspace[23].

[Case example]

○ *The United Nations (UN) Group of Governmental Experts (GGE), which has been established under the UN First Committee (governing disarmament and international security) in succession since 2004, recommended 11 norms of responsible state behavior in cyberspace*[24] *(such as that states should not knowingly allow their territory to be used for internationally wrongful acts using information and communication technologies (ICTs); states should respect human rights on the internet; states should not conduct ICT activity that intentionally damages critical infrastructure; and states should take reasonable steps to ensure the integrity of the supply chain) and confirmed that existing international law, including the entire UN Charter, is applied in cyberspace, etc. It was also determined in 2018 that the Open-Ended Working Group (OEWG), which deals with similar issues as the GGE in a separate framework, was to be established under the First Committee.*

○ *A resolution was adopted in November 2019 for the establishment within the UN of an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive*

[23] Cybersecurity Strategy (approved by the Cabinet on September 28, 2021), page 8.

[24] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (https://digitallibrary.un.org/record/799853)

international convention on countering the use of information and communications technologies for criminal purposes, apart from the Convention on Cybercrime formulated by the Council of Europe and signed by 66 countries including Japan, the United States, and Europe (as of the end of September 2021) (a.k.a. Budapest Convention; adopted by the Council of Europe in 2001 and the signing ceremony was held in the same year where Japan signed it as well). The Ministry of Foreign Affairs of the Russian Federation presented criticism stating that, for example, "existing multilateral conventions were formulated 10 or 20 years ago and are not catching up with developments of cybercrimes," and "provisions related to access to data beyond national borders have a high risk of breaching the principle of state sovereignty and other similar principles."[25]

Furthermore, as national security has been expanding its scope to economic and technological fields, the struggle for technological supremacy is also emerging[26].

[Case example]

○ *The United States announced in August 2020 its Clean Path (Clean Network) program, which is a plan to exclude untrusted business operators from communications carriers, app stores, application and cloud service vendors, and undersea cable businesses in order to protect people from malicious attackers. In addition, in June 2021, the U.S. Federal Communications Commission determined a policy to prohibit certification of communication devices of five non-U.S. companies deemed to be a risk to national security and substantially exclude them from the U.S. market. Furthermore, a draft regulation was published (public comment was invited) in October 2021 on transactions of cybersecurity products that may be exploited for cyberattacks.*

○ *Concerning undersea cables, there have been cases in which connection destinations in a plan were changed due to concerns expressed by the U.S. Government and in which an undersea cable plan related to Pacific Islands was invalidated after implementing the bid because the required conditions were allegedly not met. In addition, amid the situation where installation of undersea cables in the Arctic Ocean was attracting the attention of neighboring countries when the area of sea ice in the region was contracting, only a project of the Russian Federation alone remained with the completion of installation aimed in 2026, after an international project announced in June 2019 was put on hold in May 2021.*

[25] International Community Has Become Closer to "Cybercrime Vaccine" (https://www.mid.ru/en/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/4836268)

[26] Cybersecurity Strategy (approved by the Cabinet on September 28, 2021), page 8.

1. 3. 3 Risks of cybercrime groups, etc.

Threats of crime groups in cyberspace have been increasing on a global scale. According to a survey by a U.S. company published in May 2021[27], "criminal organizations" accounted for about 80% of the total types of attackers related to leakages and breaches globally.

Many cases concerning ransomware have actually occurred that had a large impact on people's lives.

[Case example]

○ *In May 2021, one of the largest U.S. petroleum pipeline operators was attacked by a cybercrime group using DarkSide ransomware, and its operation was suspended for about a week. As a result, fuel shortages occurred in some regions.*

○ *In May 2021, the world's largest meat processor was attacked by a cybercrime group using REvil ransomware (a.k.a. Sodinokibi) and suspended the operation of meat processing plants in the United States, Australia, and Canada for three days. As a result, meat prices surged.*

○ *In October 2021, a Japanese medical institution was attacked using ransomware, and electronic medical records of about 85,000 patients became encrypted and unavailable for browsing. As a result, the medical institution suspended acceptance of new patients requiring medical care and patients requiring emergency treatment.*

Attack methods have become more sophisticated, making it more difficult to prevent damage.

[Case example]

○ *The cases of companies in various countries worldwide falling victim to encryption from REvil ransomware in July 2021 began with a supply chain attack exploiting a zero-day vulnerability[28] in VSA, a system management service provided by a U.S. software company.*

○ *According to a questionnaire survey conducted by the National Police Agency on companies that reported damage from ransomware to the police in the first half of 2021, 13% of respondents said that the route of infection was an email or an email attachment, 55% said it was intrusion through a virtual private network (VPN) device, and 23% said it was intrusion through remote desktop, indicating the signs that attacks hit the weak points that have arisen following the rapid increase of people engaging in remote work cleverly.*

Furthermore, anti-analysis functions (functions to obstruct or delay analysis) of malware used for attacks have also been advancing. Such malware has a variety of functions, including avoiding

[27] "2021 Data Breach Investigations Report," Verizon

[28] Vulnerabilities before fixes are released

pattern matching[29] by altering source codes, encrypting character strings, and detecting analysis environments to hinder analysis by investigative agencies and security vendors, making analysis more difficult in terms of both quality and quantity, while causing the time required for implementing measures based on analysis to increase and, by extension, the damage to expand.

[Case example]

○ *Conti ransomware has anti-analysis functions such as calling a large number of meaningless application programming interfaces (APIs) and encrypting all character strings executed.*

○ *Some of the EKANS (SNAKE) ransomware has a function to operate only when it successfully connects to specific domains to avoid detection by operating in places other than the targets. Due to this function, analysis cannot be conducted unless environments similar to said targets are created.*

○ *Ragnar Locker ransomware has such functions as killing itself upon detecting that it is being analyzed.*

As described above, attacks by crime groups have become more malicious and sophisticated, and in addition, attack tools are traded on certain forum websites, etc. and a criminal infrastructure (an infrastructure to promote crimes or make it easy to perform them) has been built where anyone with a certain level of skills but who lacks special expertise, can perform cyberattacks. Furthermore, it is noted that there are not only crime groups that are directly related to attacks but also, for example, those that provide means for anonymization, such as VPN and private proxy, those that verify whether stolen credit card information is valid, and those that perform such activities as money laundering, and these groups have been broadly connected to form a sort of ecosystem.

Online meetings were held on October 13 and 14, 2021, with participants from 32 countries and regions, including Japan, the United States, Europe, and the European Union (EU), to strengthen international collaboration in countering cyberattacks using ransomware, where a joint statement was issued[30] stating that ransomware has become a more serious global threat against national security. As such, threats of cybercrime groups, etc. have become more serious on a global scale.

[29] A technique to attempt detection of malware by comparing a list of code patterns distinctive to known malware with the file subject to analysis.

[30] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021 (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/)

2 Basic principles and policy issues

2. 1 Basic principles ― Roles of the new organizations

"Japan as the Safest Country in the World" is an irreplaceable social asset. And the role that the police organization as a whole should fulfill is to foster and protect the asset.

However, the threats in cyberspace remained grave due to threats of damage from ransomware and a large number of cyberattacks. In addition, the fact that cybercrimes are ranked top as a cause of a sense of anxiety over damage from crimes[31] is also a point of concern. As stated in the "Introduction," it goes without saying that the new organizations which the National Police Agency will establish in FY2022, namely, the Cyber Affairs Bureau, which will centrally take charge of policies related to cyber incidents, and the National Cyber Unit, which is expected to take charge of international joint operations and investigations of grave cyber incidents as an investigative unit of the national government, are highly required to address threats that jeopardize the safety and security of cyberspace as public space.

Meanwhile, as discussed above, in the new society where cyberspace and real space are integrated, the damage and impact of cyberattacks are not confined only to cyberspace, and in addition, the level of threats is heightened to an unprecedented degree. Therefore, it is unrealistic to pursue safety and security in cyberspace only, but attention should be paid to threats straddling cyberspace and real space in particular.

Moreover, the new organizations should prepare measures for a variety of threats, ranging from familiar cases such as online banking fraud to the exploitation of broadband communication networks and technological innovations. Not all risks emerging in digital society as summarized in 1.3 are required to be addressed under the lead of the police, but they are believed to provide valuable points of view in understanding these wide-ranging threats and considering on what the police should work.

The new organizations are required to play a central role in ensuring the safety and security of the digital society where real space and cyberspace as public space are integrated, and they must not only address threats in full in both cyberspace and real space through a concerted effort of the police organization as a whole, in collaboration with existing police departments such as Criminal Affairs departments, Community Safety departments, Traffic departments, and Security departments, but also ensure the further safety and security of the new society in cooperation with diverse stakeholders (through a multi-stakeholder process[32]).

[31] Crime Situation in 2020 (National Police Agency)

[32] According to materials from the Cabinet Office (https://www5.cao.go.jp/npc/sustainability/concept/index.html), it is "a framework for consensus building in which a wide variety of stakeholders participate on an equal footing

Based on the preceding, the roles, or basic principles, expected of the Cyber Affairs Bureau and the National Cyber Unit shall be defined as to ensure the safety and security of the digital society where real space and cyberspace as public space are integrated, and to realize safety and security through activities of multi-stakeholders.

2. 2 Policy issues

Issues to be solved for the new organizations to fulfill their role are sorted out and classified broadly into four categories, namely, "Strengthening of the handling system" to promote measures properly; "Strengthening of international collaboration and response" to push forward with effective initiatives against the cross-border nature of cyberspace; "Strengthening of the abilities to ascertain situations and adapt to social change" to respond to an ever-changing society where new technologies and services are created on a daily basis; and "Safety and security generated by society as a whole" to push forward with initiatives based on a multi-stakeholder process.

2. 2. 1 Strengthening of the handling system

(1) Establishment of organizations capable of undertaking initiatives with an eye on ensuring the safety and security of the entire digital society

In a new society where cyberspace and real space are integrated, damage and impact of cyberattacks are not confined only to cyberspace, and the level of threats is heightened to an unprecedented degree. In view of the foregoing, it is necessary to establish new organizations aimed at ensuring the safety and security of not only cyberspace but also the entire digital society where real space and cyberspace as public space are integrated, in collaboration with existing organizations.

(2) Realization of an environment to increase competent and talented human resources and to use them flexibly

A key for an organization to function effectively is to attract and develop competent and talented human resources and enable them to play an active role.

Meanwhile, competent and talented human resources, including advanced experts, also fulfill vital roles in local regions, and it is not appropriate to simply concentrate human resources in the new organizations.

To address this situation, initiatives are needed to realize an environment to not only increase competent and talented human resources but also to use them flexibly.

and work together to solve problems," which enables development of a relationship of trust among participating stakeholders, ensuring of the validity of the consensus reached, promotion of independent initiatives undertaken by participating stakeholders, and pursuit of overall optimization. As various stakeholders are involved in cyberspace, it is necessary to promote broad collaboration among organization and individuals, not limited to specific stakeholders, to solve issues.

2. 2. 2 Strengthening of international collaboration and response

(1) Development of a robust relationship of trust with overseas public security authorities

With the cross-border nature of cyberspace, it is essential to obtain information located overseas in investigating cybercrimes. Therefore, requests to foreign countries are broadly made to obtain information possessed by providers located overseas through overseas investigative agencies based on frameworks of international cooperation in criminal investigations. In addition, as seen in takedowns of Emotet[33] and Double VPN[34], international joint operations have been undertaken in other countries, in which investigative agencies of various countries carry out joint operations by complementing investigation results of each other after proceeding with international investigations through the above-mentioned frameworks.

In Japan, while frameworks related to international cooperation in criminal investigations have been developed to a certain degree, as exemplified by the signing of the Convention on Cybercrime, there have been many cases in which international investigations do not sufficiently advance due to reasons including the length of time it takes to receive answers to requests through initiatives such as mutual legal assistance, and participation in international joint operations has been subdued due in part to a fact that there are no investigative entities engaged in international investigations on an ongoing basis.

A key in relationships with overseas public security authorities is to build a reciprocal relationship with the give and take principles in mind, including Japan not only asking counterparty agencies for cooperation but also responding to requests for cooperation from them. It is also essential to build a working-level relationship of trust among those who are engaged in investigations, with their own organizations, not to mention building ongoing relationships among organizations. In view of the circumstances as described above, it is necessary to take initiatives from the medium- to long-term perspective to build a robust relationship of trust with overseas public security authorities through steady and diligent contribution toward the building of a working-level face-to-face relationship and collection, analysis, and provision of information drawing on strengths of the police of Japan.

(2) Ensuring the safety of cyberspace in collaboration with relevant countries, etc.

[33] A malicious program that has a function to spread infection by stealing information such as the destination and body text of emails sent out or received by computer users and create and send spoofed emails based on said information and has caused significant damage on a global scale.

[34] A service which advertised that it would provide an extremely high level of confidentiality by using a maximum of 4 VPN connections and was exploited by parties who carry out ransomware attacks, phishing, etc. to mask their locations and identities.

To improve the cyberspace environment, which is said to be incredibly advantageous to attackers, and ensure its safety, it is necessary to take specific initiatives in collaboration with relevant countries, etc.

Participating in international joint operations after building a robust relationship of trust will contribute to crushing criminal infrastructures, arresting crime groups, and clarifying the actual situation in Japan and overseas.

It should also be noted that participating in international joint operations and conducting arrests and clarification of actual situations on an ongoing basis are expected to have a deterrence effect causing attackers to hesitate attacks against Japan, and in addition, if attackers are identified as a result of investigations, it will not only serve Japan’s own interest but also lead to considerable international contribution. In addition, based on the viewpoint that cyberspace has become part of a realm of interstate competition that reflects geopolitical tensions, it is important to conduct international joint operations broadly in collaboration with countries that have shared values, such as the rule of law, freedom, and democracy, and international organizations.

Furthermore, behind recent discussions on such matters as formation of international rules lie a large number of cyberattacks and extremely harsh circumstances which are said to be advantageous to attackers, and it is required that the police, who should fulfill their role in identifying attackers and clarifying actual situations, take a stance to proactively be involved in these discussions so that Japan’s principle of “thorough enforcement of the rule of law” will not be compromised.

2. 2. 3 Strengthening of the abilities to ascertain situations and adapt to social change

(1) Recognizing incidents and changes in situations at an early stage

Victimized business operators, etc., tend to hesitate to report to or consult with the police due to concerns about a reputation risk caused by disclosure of information leakage or hindrance to early recovery of business operations that might occur as they cooperate in investigations. As such, damage may be concealed, and in turn, the accuracy in understanding the situation may deteriorate.

Even recently, there have been countless cases in which new technologies and services are exploited, including illicit remittance via smartphone payment services, surrogate SMS authentication, and demanding ransom using ransomware, which exploits the anonymity of crypto-assets.

To take appropriate measures to ensure the safety and security of new society where new technologies and services are created successively and circumstances constantly change, initiatives need to be taken to recognize the occurrence of incidents and changes in situations at an early stage.

(2) Clarification of actual situations and promotion of effective countermeasures

The incident concerning JAXA in which a male Chinese Communist Party member was arrested in April 2021 is an example where it was unraveled that Unit 61419 of the Chinese People's Liberation Army was highly likely to be behind the incident, and, further, where the expansion of damage was prevented because the police provided information promptly to victimized companies, etc. on their possible infection with a malicious program and effective countermeasures individually. In addition, in July 2021, Japan's Foreign Press Secretary issued a comment[35] firmly condemning malicious cyber activities concerning cyberattacks conducted by cyberattack group APT40, which the Chinese government is highly likely behind. Results from initiatives to deter cyberattacks by disclosing and condemning attackers through public attribution[36] like this are steadily bearing fruit, and initiatives need to be taken to clarify actual situations and further promote effective countermeasures, including comprehensive analysis and evaluation of wide-ranging related information and uncovering state involvement.

2. 2. 4 Safety and security generated by society as a whole

(1) Measures, etc. to prevent new technologies and services from being used as a criminal infrastructure

New technologies and services are sometimes exploited by criminals and function as a criminal infrastructure in ways such as demanding ransom via ransomware, which exploits the anonymity of crypto-assets, and phishing by disguising a communication concerning the delivery status of an order via SMS.

In addition, in a society where new technologies and services are successively created, it is expected that there will be a further rise in the number of cases where a technology that is initially considered to be safe and becomes broadly common, comes to be exploited by using a loophole in the system and serves as a criminal infrastructure, as seen in surrogate SMS authentication.

Measures need to be taken to allow people in charge of system design, services design, technology development, and research to work together and prevent new technologies and services intended to benefit people from being used as a criminal infrastructure.

(2) Fostering a foundation for ensuring safety and security by the entire community

[35] Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html)

[36] Activities to disclose and condemn attackers identified through attribution (activities to identify the perpetrator and its techniques and purposes) and thereby deter cyberattacks

While the police has strengths in its activities closely tied to local communities undertaken through the Prefectural Police Headquarters and numerous police stations and police boxes, it is absolutely impossible that the police bear the responsibility for the safety and security of new society alone.

It is indispensable for everyone to be aware of their responsibility for ensuring safety and security and to raise the tide for creating a safe and secure society together, and initiatives need to be taken to foster such a foundation.

In addition, in undertaking public awareness campaigns, it is also essential to consider not only a viewpoint of literacy aiming to acquire knowledge but also viewpoints of awareness aiming to form habits and consciousness related to security and of competency aiming for obtaining an ability to harness knowledge.

3 Specific measures

Now that the recognition of circumstances has been presented and the basic principles, etc. expected of the new organizations in addressing such circumstances have been sorted out, next, major examples of measures will be presented below which are required or expected to be taken by the Cyber Affairs Bureau, etc. to solve policy issues sorted out above.

These include a wide variety of measures such as those to promote or strengthen existing initiatives on an ongoing basis, those requiring to be worked on at the same time when or promptly after the new organizations are set up, those requiring new budget, and those requiring medium- to long-term consideration. As such, it is essential to promote, in particular, individual measures requiring medium- to long-term consideration and initiatives in a planned manner by, for example, preparing a roadmap from a panoramic viewpoint covering a certain period of time.

In addition, in promoting such measures, it is important to secure resources in terms of systems, budget, etc. for promoting initiatives on an ongoing basis.

Furthermore, not all of the measures listed below may always be realized by cyber departments alone. Rather instead, collaboration with relevant ministries and agencies, industry-academia stakeholders, etc., including other departments within police departments and the National Center of Incident readiness and Strategy for Cybersecurity, is the key to the realization. As such, it is also indispensable to have a perspective of encouraging stakeholders to work as one under the concept of a multi-stakeholder process.

3. 1 Strengthening of the handling system

I–1 Establishment of organizations capable of undertaking initiatives with an eye on ensuring the safety and security of the entire digital society

(i) Building a system for sophisticated analysis related to cyber incidents

The Cyber Affairs Bureau, which is to be established in FY2022, is required to address various threats ranging from familiar threats emerging in cyberspace to threats exploiting broadband communication networks and technological innovations. Information serves as the basis for incident response and policy formulation. Accordingly, a system for sophisticated information analysis, in particular, will be established within the Cyber Affairs Bureau, and the following initiatives will be promoted.

○ Diverse information will be analyzed, including cyber-related information within the police, in preparation for broad use, from clarification of actual situations to measures to prevent damage, as well as information provided by other organizations and private companies.

○ Analysis, etc. of newly emerged risks will be promoted by strengthening collaboration with business operators who face and/or address new risks on a daily basis and consumers' associations, etc., which collect voices of consumers, through such means as collecting anecdotal information from them.

○ Analysis and evaluation of the scope of impact of cyberattacks, etc., and where the impact would occur will be promoted in collaboration with relevant agencies, as it has become difficult to predict the foregoing due to supply chains, etc. becoming more complex and obscure.

(ii) Building a system for collaboration with other departments, etc. within the police

To address threats in full in both cyberspace and real space, it is necessary to build a system for effective collaboration with other departments, including Community Safety, Criminal Affairs, Traffic, and Security departments, or between the National Police Agency and the Prefectural Police departments. Therefore, the following initiatives will be promoted.

○ A collaborative system will be built in FY2022 between the Cyber Affairs Bureau of the National Police Agency and other departments, including Community Safety, Criminal Affairs, Traffic, and Security Bureaus, to share information and provide mutual support for policy formulation and technical advice, assistance, etc.

○ Collaboration will be strengthened in FY2022 by, for example, providing technical support from cyber departments to other departments and enhancing information sharing among departments so that the Prefectural Police departments can also address crimes exploiting new technologies and services, crimes straddling real space and cyberspace, etc. appropriately.

○ In order for the National Cyber Unit to achieve results, close collaboration with the Prefectural Police departments is indispensable. As such, roles to be shared will be clarified to prevent any gap from occurring within the police while taking into account differences in the handling abilities of the respective Prefectural Police departments, and the forms of collaboration will be reviewed constantly to ensure them to be optimal for the police organization as a whole in view also of such matters as how the handling abilities of the Prefectural Police departments have been strengthened.

○ Efforts will be made to provide information on the sharing of roles among the Cyber Affairs Bureau, other departments of the National Police Agency, the National Cyber Unit, and the Prefectural Police departments to business operators, etc. appropriately.

(iii) Promotion of research and study related to systems, initiatives, etc. of other countries

To maintain and develop abilities to formulate and implement policies effectively and proactively, it is necessary to learn from advanced initiatives, trends in the reorganization, etc. of other countries and review our measures as necessary. Accordingly, research and study related to systems, initiatives, etc. of other countries will be promoted on an ongoing basis.

I–2 Realization of an environment to increase competent and talented human resources and to use them flexibly

(i) Securing talented human resources

For the Cyber Affairs Bureau and the National Cyber Unit to fulfill their functions fully, it is indispensable to secure and use diverse, competent, and talented human resources. Therefore, the following initiatives will be promoted on an ongoing basis.

○ Efforts will be made to hire people who are particularly expected to have the talent to become advanced experts from colleges of technology, universities, etc. which have strong advantages in the information field.

○ To ensure the diversity of human resources, technical personnel will be recruited simultaneously with technology departments other than analysis departments, and external human resources will be hired proactively as expert investigators[37].

(ii) Enhancing and strengthening development and improving treatment of advanced experts and expert investigators

For secured talented human resources to demonstrate their abilities fully, it is necessary to develop them in a planned manner by, for example, allowing them to have opportunities to be exposed to the latest knowledge, etc., and it is also necessary to improve their treatment so that they can play an active role with high morale. Therefore, the following initiatives will be promoted.

○ Measures will continue to be promoted, such as dispatching human resources to the Japan Cybercrime Control Center (JC3), private companies, etc., providing lecture courses, etc. by technical advisors on cybercrime countermeasures[38] to investigators, and utilizing private-sector training using advanced training facilities.

○ In FY2022, a human resource development platform will be created that enables remote access to advanced training environments, etc., and efforts will be made to increase opportunities to receive advanced and practical training also in local regions and improve the contents of intradepartmental training on an ongoing basis.

○ In FY2022, with respect to national tournaments related to cybersecurity for advanced experts, expert investigators, etc., which have previously been held separately, consideration will be

[37] Investigators who have a high level of knowledge in addressing cybercrimes and cyberattacks, including cybercrime investigators who are a mid-career hire or special hire employed on the condition of having experience in private companies and/or a high level of qualifications related to information and communications technology.

[38] Experts such as personnel of companies related to information communications and university professors who are appointed by a Prefectural Police department and provides required advice, etc. on knowledge and technology related to cybercrime investigations and countermeasures.

given to establishing new competitions among teams consisting of both such experts and investigators, and in addition, efforts will be made to increase talented human resources who are conversant with both investigation and analysis by promoting human interaction and sharing of knowledge through such means as continuously allowing them to participate in mutual training programs.

○ Efforts will be made to create an environment where advanced experts can readily play an active role by, for example, establishing career tracks where human resources with an extremely high level of specialized skills can serve in the same post over the long term or in a post related thereto and accumulate and make use of advanced technological knowledge so that they can have an opportunity to play an active role commensurate with their abilities, and considering to give them incentives such as avoiding relocation for work through the use of an analysis platform to be developed in FY2022 which realizes remote analysis and mutual support.

(iii) Raising the level of handling abilities of police personnel as a whole

In view of the situation where understanding and awareness of cybersecurity and abilities to master digital technology are required at all departments, cultivating these abilities is positioned as an important foundation in training[39], like kendo and judo, and identified as priority fields to expand the human resource pool. Accordingly, the following initiatives will be promoted.

○ As part of measures to support self-improvement, sharing of training materials prepared by the National Police Agency to the Prefectural Police departments will be promoted in FY2021, and consideration will be given in FY2022 to enhancing tournaments within police departments related to cybersecurity.

○ In FY2022, the human resource development plan will be reviewed to stress the importance of cultivation related to cybersecurity, etc., and consideration will be given to such matters as the review of training contents to effectively use training opportunities arranged for such occasions as the time of recruitment, promotion, etc., an increase in training opportunities, and the development of training materials for trainees in the new recruit training course.

(iv) Creation of an environment for the flexible use of competent and talented human resources

Competent and talented human resources placed across Japan have been taking charge of operations such as analysis related to investigations undertaken by various departments, including cyber departments. It is certain that demand such as demand for advanced analysis

[39] According to a concept statement announced by the Digital Agency in relation to the JAPAN DIGITAL DAYS 2021, there are moves toward undertaking initiatives by “considering the principle of how individuals and organizations should use digital technology as ‘Digi-do (tentative name)’ (‘do,’ as used in kendo and judo, means a pursuit of the ideal form in the specific field).”

associated with the establishment of the Cyber Affairs Bureau and the National Cyber Unit, demand for investigations undertaken by cyber departments themselves, and demand for providing technical support to other departments will significantly increase in the future. To meet these demands, it is necessary to flexibly create an environment for using competent and talented human resources. Therefore, the following initiatives will be promoted.

○ In FY2022, an analysis platform will be developed which realizes remote analysis and mutual support, and in addition, efforts will continue to be made to improve the performance and strengthen the functions of material and equipment.

○ Building and enhancement of systems will continue to be promoted so that routine analysis, etc. may be conducted within the Prefectural Police cyber departments, and thereby, advanced experts may focus on more advanced analysis.

3. 2 Strengthening of international collaboration and response

II–1 Development of a robust relationship of trust with overseas public security authorities

(i) Dispatching and placement of personnel to overseas public security authorities

To build a relationship of trust with overseas public security authorities, it is indispensable to dispatch our personnel and build a face-to-face relationship with them. Therefore, the following initiatives will be promoted.

○ Officers in charge of overseas communications (liaisons) will be dispatched to Europe in FY2022 to promote daily information exchange and the building of face-to-face relationships.

○ Consideration will be given to career tracks (placement to a post over the long term, to an appropriate post, etc.) of personnel who are dispatched and enhancing dispatch of personnel to overseas public security authorities, taking into account examples of other countries.

(ii) Holding of international meetings inviting personnel of overseas public security authorities and participation in international conferences

To build a relationship of trust with overseas public security authorities, it is also effective to deepen mutual understanding through such means as periodic meetings and establish a prominent position in events and similar assemblies. Therefore, the following initiatives will be promoted.

○ Participation in international private-sector events and similar assemblies will continue to be made, our prominent position will be demonstrated by showcasing the high level of technological prowess of the police’s advanced experts, and a foundation will be fostered to build relationships with overseas public security authorities.

○ Information exchange from both investigation and technological aspects and working-level mutual understanding, relationship building will be promoted through such means as holding of international meetings inviting personnel of overseas public security authorities starting from FY2022 and continued participation in international meetings held by other countries.

(iii) Ongoing promotion of existing collaborative frameworks such as mutual legal assistance

In order to build a relationship of trust with overseas public security authorities, it is effective to not only build a face-to-face relationship among individuals but also repeat cooperation and reciprocation among countries (or organizations). Therefore, the following initiatives will be promoted.

○ Appropriate responses will continue to be promoted concerning requests from other countries for mutual legal assistance. Specifically, following the establishment of the National Cyber Unit, the national government will directly be involved in responses to requests, the handling of which has previously been relied on the Prefectural Police departments. This will enable swift and accurate handling of requests even further, and improvement of international trust will also be pursued through such efforts.

○ Efforts will continue to be made to develop and maintain a close and collaborative relationship with overseas public security authorities, which will be particularly important in public attribution.

II–2 Ensuring the safety of cyberspace in collaboration with relevant countries

(i) Promotion of strategic international investigations by the National Cyber Unit

With the cross-border nature of cyberspace, international investigations are indispensable when investigating cybercrimes. Starting from FY2022, the National Cyber Unit will come to the forefront and promote international investigations strategically as an investigative agency of the national government. Proactive participation will be made in international joint operations related to disrupting international cybercrime groups, criminal infrastructures straddling multiple countries, in particular, providing work products based on investigation-related information collected by the Prefectural Police departments and results of analysis by advanced experts as a footing for the participation, in reference to such matters as initiatives of other countries which have already been involved in the operations.

(ii) Proactive involvement in international discussions on such matters as formulation of international rules

To improve the cyberspace environment, which is said to be advantageous to attackers, it is necessary to work to not only disrupt criminal infrastructure through investigations but also promote the rule of law in cyberspace through international discussions. Generalization and improvement of the contents of conventions will continue to be promoted by using existing international frameworks, including the Convention on Cybercrime, through such efforts as providing information regarding results of analysis on circumstances of threats such as cyberattacks which a state is behind, international affairs that have been a hindrance to investigations to relevant ministries and agencies appropriately.

In addition, proactive involvement in international discussions will be made, such as full involvement in discussions at the UN related to the formulation of a new convention for which the first meeting of open-ended ad hoc intergovernmental committee of experts is planned to be held in January 2022.

3. 3 Strengthening of the abilities to ascertain situations and adapt to social change

III–1 Recognizing incidents and changes in situations at an early stage

(i) Raising the tide for promotion of reporting to and consulting with the police

In order to take appropriate measures to ensure the safety and security of a new society where new technologies and services are created successively and circumstances change constantly, it is necessary to recognize incidents and changes in situations at an early stage. To do that, it is indispensable that suffered damage is reported to and consulted with the police so that damage would not be covered up. Currently, however, it is believed that many cases involving damage by cybercrimes have been covered up, as victimized companies do not report to or consult with the police due to concerns such as a reputation risk or hindrance to early recovery of business operations caused by investigations.

In this context, in line with the statement in the Cybersecurity Strategy that "by […] encouraging victims of cybercrimes to report to the police and notify public agencies, the national government will eliminate factors and environments that tolerate cybercrimes,"[40] the police will continue to undertake public awareness campaigns to promote reporting of damage and work to raise the tide for promotion of reporting and consultation in collaboration also with private business operators.

(ii) Improvement of an environment to enable smooth reporting to and consultation with the police

To promote reporting to and consultation with the police, it is indispensable for the police to not only undertake public awareness campaigns but also improve a reporting and consultation friendly environment in response to concerns of companies, etc. which have been an obstacle to reporting and consultation and complaints about defective handling on the side of the police. Therefore, the following initiatives will be promoted.

○ There are companies, etc. concerned about reputation risks and hindrance to early recovery of business operations caused by investigations. As such, in FY2022, consideration will be given

[40] Cybersecurity Strategy (approved by the Cabinet on September 28, 2021), page 19.

to how initial investigations for cybercrimes should be conducted so that they are conducted with consideration for victimized companies, etc. to the extent possible.

○ There have also been complaints about defective handling by the police after receiving reports and consultations. Accordingly, as stated in I, starting from FY2022, readiness will be expedited to handle them more appropriately by raising the level of cybersecurity literacy for police personnel as a whole and implementing interdepartmental collaboration. In addition, consideration will be given to the improvement of consultation handling and the ideal form of public-private collaboration to realize more appropriate and smooth handling.

○ There have also been remarks that a person in charge at or business manager of a victimized company may not come up with the idea of reporting to or consulting with the police when they suffered damage. Therefore, consideration will be given to measures to promote risk communication with persons in charge at companies, etc. at normal times.

(iii) Improvement and advancement of analysis of consultations related to cyber incidents and early communication within police departments

To recognize changes in situations early and appropriately, it is necessary to promptly consolidate information obtained through reports and consultations and analyze it as a whole, instead of each piece of information. Therefore, the following initiatives will be promoted.

○ Starting from FY2022, analysis will be conducted on information obtained through reports and consultations from a panoramic viewpoint, together with investigative information, etc. consolidated to the analysis system established within the Cyber Affairs Bureau as stated in I–1 from across Japan.

○ Consideration will be given to operations related to information communication to allow information obtained by police stations, etc. through consultations is shared with the Police Headquarters and the National Police Agency swiftly and used for analysis within the police stations, etc.－Police Headquarters－National Police Agency structure.

(iv) An increase in and improvement of joint handling with business operators

It is also necessary to put measures in place to recognize incidents and changes in circumstances other than reporting and consultation. In this context, while currently there is a possibility that damage from cyber incidents may occur regardless of the company size or industry, it is effective to build relationships with a broader range of business operators than ever before and strengthen existing collaborative relationships. Therefore, the following initiatives will be promoted.

○ Starting from FY2022, efforts will be made to promote the execution of joint handling agreements aiming to prevent cybercrime damage cases from being covered up or recurring with not only financial institutions, which account for the majority of victims at present, but also companies in wide-ranging industries, including small and medium-sized enterprises (SMEs) and local industrial organizations such as commercial and industrial associations. In addition, even after executing such agreements, efforts will be made to improve the effectiveness by, for example, building a face-to-face relationship in normal times.

○ In FY2022, consideration will be given to more practical forms of collaboration to strengthen collaboration with security vendors who play a key role in ensuring the safety and security of cyberspace together with the police, software developers who face risks of vulnerabilities in their software being explored and exploited, and cloud service providers who provide indispensable infrastructure in cyberspace and have become an important actor in ensuring the security following the advancement of Secure Access Service Edge (SASE)[41].

○ Efforts will continue to be made to closely collaborate with business operators in the event of incidents.

III–2 Clarification of actual situations and promotion of effective countermeasures

(i) Improvement and sophistication of analysis of investigation-related information, etc. concerning cyber incidents and promotion of crackdowns

When incidents are recognized through reports, consultations, etc., it is indispensable to have a perspective of seeking to unravel the criminal techniques, etc. and prevent the expansion of damage, in addition to arresting suspects. Therefore, the following initiatives will be promoted.

○ Efforts will continue to be made to clarify actual situations in a broader scope by, for example, instead of focusing on one incident only, analyzing and evaluating other wide-ranging related information comprehensively and uncovering involvement of a specific attack group, state institution, etc. in a cyberattack, and to push forward with crackdowns of cyber incidents and disclose unraveled information appropriately.

○ Efforts will continue to be made to analyze investigation-related information, etc. from a broader viewpoint, in consideration also of prevention of expansion of damage, measures against criminal infrastructures, etc. As damage from ransomware, in particular, has a massive impact on various industries, initiatives will be promoted to analyze cyber incidents and prevent recurrence and expansion of damage in conjunction with relevant government agencies, organizations, etc.

(ii) Sophistication and efficiency improvement of analysis for attribution

[41] A concept in which security functions and network functions are integrated into a single cloud service.

It is effective to promote clarification of actual situations and countermeasures through attribution for incidents, the suspects of which are significantly difficult to arrest, such as cyberattacks behind which is a specific group, state institution, etc. Therefore, the following initiatives will be promoted.

○ Efforts will continue to be made for improvements in efficiency and sophistication of analysis by expediting analysis readiness through machine learning and other means to address issues such as diversification of malware and implementation of anti-analysis functions.

○ While many human resources have been invested in such efforts as comprehensive analysis of a large amount of data, including indicators of compromise (IoCs)[42] and verification of the data relativity, which are indispensable for attribution, starting from FY2022, consideration will be given to the introduction of AI to promote improvement of efficiency in this kind of work and enable investment of human resources in more advanced analysis, judgment, etc.

The use of AI should be made after appropriate consideration and under appropriate measures based on the "Social Principles of Human-Centric AI" (approved by the Council for Integrated Innovation Strategy on March 29, 2019), etc.

○ It is necessary to collect IoCs efficiently to appropriately respond to a large number of cases of damage, which has been covered up, coming to the surface through the promotion of reporting and consultation. Consideration will be given to methods of the collection, along with the creation of an environment that allows smooth reporting to and consultation with the police.

(iii) Collection and sophistication of analysis of threat information, etc. on the internet

It is also effective to collect information that would contribute to clarification of actual situations and address illegal and/or harmful information on the internet as measures to prevent damage or expansion of damage. Therefore, the following initiatives will be promoted.

○ Proactive promotion of initiatives will be continued, including accusations and requests for deletion, to take strict actions against illegal and/or harmful information such as child pornography, ads for controlled substances, and instigation to commit suicide, using reports from the Internet Hotline Center Japan as trigger information.

○ In FY2022, demonstration projects related to the exploration and analysis of illegal and/or harmful information in cyberspace using cutting-edge technology will be implemented, and consideration will be given to the introduction of AI in said area.

[42] Indicators of compromise are information that indicates traces of cyberattacks such as IP addresses and hash values.

○ Functions of the Real-time Detection Network System, which collects and analyzes threat information on the internet and the renewal of which is planned in FY2023, will be strengthened so that it can detect and identify signs, etc. of crimes actively and provide information that would contribute to crimes investigations as well as clarification of actual situations and countermeasures through attribution.

3. 4 Safety and security generated by society as a whole

IV–1 Measures, etc. to prevent new technologies and services from being used as a criminal infrastructure

(i) Provision of information to and encouragement for service providers, etc.

To prevent new technologies and services from being exploited as criminal infrastructures, it is necessary to take actions including providing information, such as the risk of exploitation and the reality of damage to service providers according to their individual and specific services and encouraging them to take necessary measures, as well as ascertaining the reality of damage and considering effective measures in collaboration with relevant organizations, etc.

Moreover, now that everyone is using the internet, there have been many incidents where victims suffer an economic loss due to exploitation of internet banking and cashless payment services or emotional distress due to slander and libel made on the internet, and thus, appropriate measures are required.

Measures against cases such as the following, in particular, where many damage cases are still being confirmed, will continue to be strengthened.

○ As part of measures against cybercrimes related to internet banking and cashless payment services, alerts concerning criminal techniques will be issued and requests to consider freezing of destination accounts for illegal remittance will be made to financial institutions, funds transfer service providers, etc.

○ With respect to surrogate SMS authentication, information on the reality of damage will be shared with relevant industry associations, etc., and consideration will be given to the necessity of obligating identity verification at the time of entering contracts for data SIM cards with an SMS function.

○ When receiving consultations related to slander and libel made on the internet, relevant departments will collaboratively handle cases according to the details and take measures necessary to relieve the anxiety of claimants by, for example, providing instructions and advice and indicating the office in charge of promoting human rights at the Legal Affairs Bureau or dedicated institutions such as the Illegal Harmful Hotline. In cases where acts violating criminal laws and regulations are identified, the police will handle the criminal cases appropriately as an investigative agency.

○ Following the widespread use of cashless payment services, as credit card information is now linked to various services, the amount of damage from unauthorized use of credit cards has been increasing[43]. Accordingly, efforts will be made to ascertain the reality of damage from incidents of unauthorized use of credit cards related to electronic commerce (EC) in collaboration with relevant organizations, etc., and consideration will be given to effective measures based on the reality of damage.

○ With respect to intellectual property, consideration and measures will be promoted on various issues that are currently obstructing investigations, based on discussions by the government as a whole, and efforts will be made to collaborate with relevant agencies, including the Cabinet Office, while working on crackdowns and prevention of damage.

(ii) Encouragement for relevant organizations to prevent expansion of damage

Under the situation where services are increasingly linked together, there is a risk that infrastructure- or platform-like services used for providing services to users are exploited as criminal infrastructures. Accordingly, it is necessary to provide information such as the risk of exploitation of services, etc. and the reality of damage to not only business operators who provide services to users directly but also business operators of such services, and encourage them to take necessary measures such as reviewing their services and ensuring the traceability.

Measures against cases such as the following, in particular, where many damage cases are still being confirmed, will continue to be strengthened.

○ Information of phishing websites, etc. obtained by the police using frameworks including public-private collaboration such as the JC3 will be provided to business operators such as antivirus software developers.

In addition, concerning SMS phishing in particular, which is a technique to mislead victims to phishing websites using text messages, relevant business operators will be encouraged to take actions to cut off such text messages guiding to phishing websites, and consideration will be given in collaboration with the JC3 to the proactive provision of investigation-related information, etc., which is necessary for initiatives of relevant business operators.

○ With respect to the transfer of crime proceeds using crypto-assets[44], industry associations will be encouraged, in collaboration with the Financial Services Agency, to take measures to

[43] Status of Occurrence of Damage From Unauthorized Use of Credit Cards (Japan Consumer Credit Association, September 2021)

[44] According to Threats in Cyberspace in the First Half of 2021 (National Police Agency, September 9, 2021), page 5, crypto-assets account for 90% of the methods for paying money demanded in relation to ransomware.

freeze destination accounts of crypto-assets used for remittance of crime proceeds, in view of the fact that measures for freezing destination bank accounts related to the remittance of crime proceeds have been taken as part of measures against crimes such as online banking fraud, and in addition, public awareness campaigns will be carried out in collaboration with business operators and others toward deterrence of damage from ransomware, etc.

(iii) Strengthening of collaboration with the JC3, security vendors, research institutions, etc.

Cooperation has been made by the JC3, security vendors, research institutions, etc. through such measures as the provision of analysis results and advanced technical information drawing on strengths of each stakeholder, including the clarification of the actual situation in the structure for division of work in remittance fraud crimes related to internet banking. In FY2022, consideration will be given to measures to strengthen the collaboration, such as establishing rules necessary for further promoting information sharing, including expansion of information provided by the police.

(iv) Takedowns of identified criminal infrastructures

Efforts will continue to be made to ensure the implementation of takedowns by providing information to administrators, etc. of criminal infrastructures such as command-and-control servers (C2 servers)[45] identified through such measures as analysis of malicious programs used in cyberattack incidents and making requests to take actions against them.

IV–2 Fostering a foundation for ensuring safety and security by the entire community

While not only the police but also diverse stakeholders have been building frameworks and working on various initiatives related to improving cybersecurity in their communities, efforts will be made to strengthen the collaboration among such existing frameworks to take measures more efficiently and effectively as society as a whole.

(i) Development of security human resources linked with school education

There have been remarks that there is a significant shortage in security human resources in local regions and SMEs in particular. For the police to contribute to their development and work to improve the defense capabilities of society as a whole, initiatives will continue to be promoted, such as dispatching instructors to and holding lectures at universities, colleges of technology, etc., using knowledge of the police related to cybersecurity.

(ii) Increase in and facilitation of cybercrime prevention volunteers

Cybercrime prevention volunteers have already been contributing to the safety and security in their communities in aspects such as education and awareness-raising activities for children,

[45] Servers that act as the center of control and send orders to devices infected by a malicious program and cause them to operate accordingly.

the elderly, etc., and cleansing of the environment through cyber patrol. Needs for and expectations of them are rapidly increasing under the situation where all people are now involved in cyberspace[46]. To respond to this situation, the following initiatives will be promoted.

○ Efforts will continue to be made to increase and facilitate cybercrime prevention volunteers even further through such measures as introducing example activities carried out in collaboration with relevant ministries and agencies, etc.

○ Awareness-raising activities about cybersecurity matters requiring attention will be undertaken for children who will lead the next generation, in collaboration with relevant ministries and agencies, by, for example, strengthening the collaboration between elementary schools and junior high schools and cybercrime prevention volunteers.

○ Efforts will continue to be made for facilitation by providing incentives such as improving the expertise of activity participants through, for example, training opportunities established for cybercrime prevention volunteers by technical advisors on cybercrime countermeasures who have previously been providing lecture courses and advice on investigations and countermeasures to investigators.

(iii) Linkage with crime prevention activities by each stakeholder rooted in communities

It is noted that sufficient actions have not been taken against threats in cyberspace at SMEs, etc., in particular. Under such circumstances, the police will continue to promote public awareness campaigns for SMEs, etc., in collaboration with property and casualty insurance companies, etc. engaging in crime prevention activities rooted in their communities to improve cybersecurity and providing cyber insurance products.

(iv) Continuous promotion of initiatives related to public-private collaboration

Initiatives related to public-private collaboration will continue to be promoted, such as the provision of threat information and advice through the Cyber Terrorism Countermeasure Councils, the Cyber Intelligence Sharing Network, etc., implementation of joint training for responses in preparation for incidents, information sharing related to cyberattacks as well as unknown malicious programs, illegal connection destinations, etc.

[46] The Cybersecurity Strategy (approved by the Cabinet on September 28, 2021) states in page 18 that “the government will advance countermeasures against cybercrime in which public and private sectors collaborate with each other in information sharing and analysis, prevention of damage due to cybercrime, and human resource development. To prevent damage from cybercrime by encouraging each individual to take voluntary measures, the government will collaborate with related institutions and organizations, including volunteer groups engaged in cybercrime prevention, and advance public awareness campaigns.”

Conclusion

The 2021 Cybersecurity Policy Council had broad discussions under the theme of the "policy package to be worked on by the new organizations including the Cyber Affairs Bureau" and summarized them in this Report.

This Report indicates that, under the situation where the establishment and use of new technologies and infrastructures such as digitalization, 5G, and satellite constellation are advancing, society is making progress from the phase of "cyberspace gaining an increasingly public nature" toward the realization of a "society where real space and cyberspace as public space are integrated," and accordingly, not only benefits but also new risks have been emerging.

Based on the foregoing, this Report reconfirms the starting point, that is, the role that the police organization as a whole should fulfill is to foster and protect "Japan as the Safest Country in the World," which is an irreplaceable social asset. At the same time, this Report clarifies that the Cyber Affairs Bureau and the National Cyber Unit of the National Police Agency are required to play a central role in realizing "the safety and security of a digital society where real space and cyberspace as public space are integrated through activities of multi-stakeholders" in cooperation with not only existing departments within the police but also diverse stakeholders.

In addition, issues to be solved to fulfill the role are sorted out and classified broadly into four categories, namely, "Strengthening of the handling system" to properly promote measures; "Strengthening of international collaboration and response" to push forward with effective initiatives against the cross-border nature of cyberspace; "Strengthening of the abilities to ascertain situations and adapt to social change" to respond to an ever-changing society where new technologies and services are created daily; and "Safety and security generated by society as a whole" to push forward with initiatives based on a multi-stakeholder process, and measures that should be undertaken to solve each of the issues are presented.

In a "society where real space and cyberspace as public space are integrated," the Cyber Affairs Bureau and the National Cyber Unit will bear the heavy responsibility as mission-critical entities for Japan to remain as the safest country in the world in the future. At the same time, it must always be borne in mind that not all measures referred to may be realized by cyber departments alone within the police, but rather, that an all-out effort should be made with stakeholders, including other departments within the police and relevant agencies of the government, industry, and academia, based on the idea of the multi-stakeholder process.

It is strongly expected that the steady implementation of the proposals in this Report and the establishment of the Cyber Affairs Bureau and the National Cyber Unit as truly effective organizations fulfilling their roles will lead to not only the safety of new society to be realized in the future but also the realization of a digital society where people can live with a sense of security.

In addition, various issues are expected to arise even after the new organizations are launched and while they push forward with specific initiatives. As the embodiment of a place where multi-stakeholders are mobilized, the Cybersecurity Policy Council is committed to continuing discussions toward developing solutions.

Preface

It is not an overstatement to say that, in recent years, cyberspace has become a space capable of broadly substituting key social and economic functions of physical space, as exemplified by a significant shift many of our social and economic activities have made to non-face-to-face and contactless activities conducted through cyberspace, due to the development of information and communications technology and the advancement of digitalization in society, such as IoT and artificial intelligence. Under such circumstances, people are suffering continuous significant damage from remittance fraud related to internet banking, committed using such techniques as by guiding victims to a phishing website through an SMS, etc., or by pretending to be a financial institution, etc.; and damage caused by ransomware to hospitals interfering with their medical care operations. Such damage affects the daily lives of people who are thus largely concerned. As described above, the positioning of cybersecurity is at a tipping point, and how we are going to protect precisely every individual in society, in addition to critical infrastructure, is probably being called into question.

The Cybersecurity Policy Meeting has taken over from the "Comprehensive Security Measures Conference" established in 2001, considered for 20 years how industries, etc. and the police should collaborate to address threats in cyberspace, and summarized the results into reports on each occasion. The Meeting advised in FY2020 that it was necessary to place "ensuring safety as a public space" as a new fundamental principle for future cybersecurity. I was profoundly moved by the fact that the National Police Agency has, based on the advice, reached a commitment to the upcoming reorganization to address the dire circumstances.

In the current fiscal year, the Cybersecurity Policy Meeting has carried over the discussions in the preceding fiscal year and considered and discussed principles to be applied and specific measures to be undertaken by the newly established Cyber Affairs Bureau and National Cyber Unit, after identifying emerging risks, etc. broadly.

The Meeting members who participated in the discussions have provided their opinions proactively from the people's perspective and on a neutral and equal footing based on their insight in their respective affiliated organizations and specialized fields. As a result, the Report was able to cover wide-ranging content.

I hope that this Report will aid in the realization of a digital society where people can live with a sense of security thanks to the facts not only that the Cyber Affairs Bureau and the National Cyber Unit function as truly effective organizations but also that these are shared with industry-academia-government stakeholders and utilized in initiatives undertaken by diverse stakeholders.

Chairperson of the Cybersecurity Policy Meeting