Section 2 Responses to Already Apparent Challenges

As described above, at a time when ICT is playing an increasingly significant role in social and economic activities, some challenges associated with the rapid penetration of ICT are already emerging, which Japan and other countries are responding to. Of these challenges, (i) risks involved in changes in the international environment, (ii) data governance, and (iii) illegal and harmful information, will be discussed in Section 2 and existing activities to respond to those challenges will be reviewed.

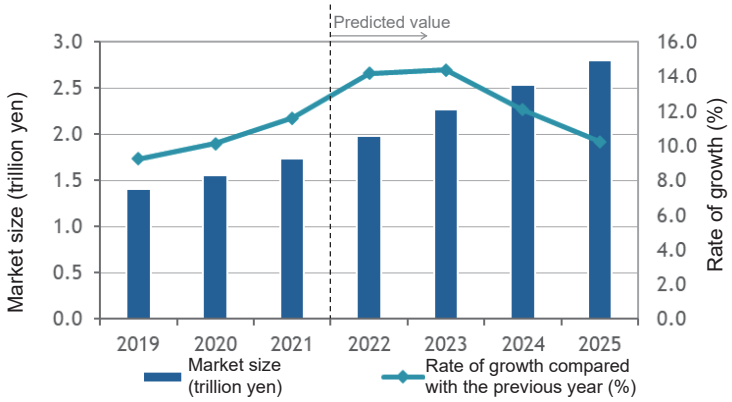
1. Response to risks involved in changes in the international environment

As discussed in Chapter 1, Section 5, amid increasingly complicated international situations in recent years, inherent risks have come to be recognized, such as the vulnerability of basic infrastructure and supply chains that form the foundation of people's lives and economic activities. In the meantime, ICT, like energy, has become the most basic infrastructure elements that support all sorts of social and economic activities, including the activities of other industries, along with the progress in digitalization in society as a whole. Therefore, it is an important task to strengthen ICT infrastructure and supply chains for ICT-related equipment and components, to secure the stable supply of ICT services and to enhance communications networks.

In recent years, there have been cases in which malware or other illegal software programs have penetrated networks through supply chains related to the procurement of equipment or systems for communication that are part of the information and communications infrastructure or related to system maintenance or operation, and there have also been cases in which supply chain security has been undermined through vulnerable organizations. There have also been cases in which the development of ICT networks has been delayed as a result of a global semiconductor shortage caused by the impact of the COVID-19 pandemic.[9]

In line with future growth in data demand due to the spread of the practical application of digital technology in rural areas, for example, the importance of data centers which store and process data is expected to grow further. Given that prospect, excessive dependence on data centers located in other countries would entail the risk of data leakage and access disruption. Around 60% of all data centers in Japan are located in the Tokyo metropolitan area (Tokyo, and Saitama, Chiba and Kanagawa Prefectures), and the predominant concentration of data centers there is expected to continue in the future. Considering the possibility that damage caused by a major earthquake or other disaster in the Tokyo metropolitan area may have a huge impact on the communications environment on a nationwide scale, it is essential to geographically disperse data centers in order to strengthen the resilience of Japanese communications networks against disasters.

Figure 2-2-1-1 Changes and forecasts for the size (sales) of the data center service market in Japan



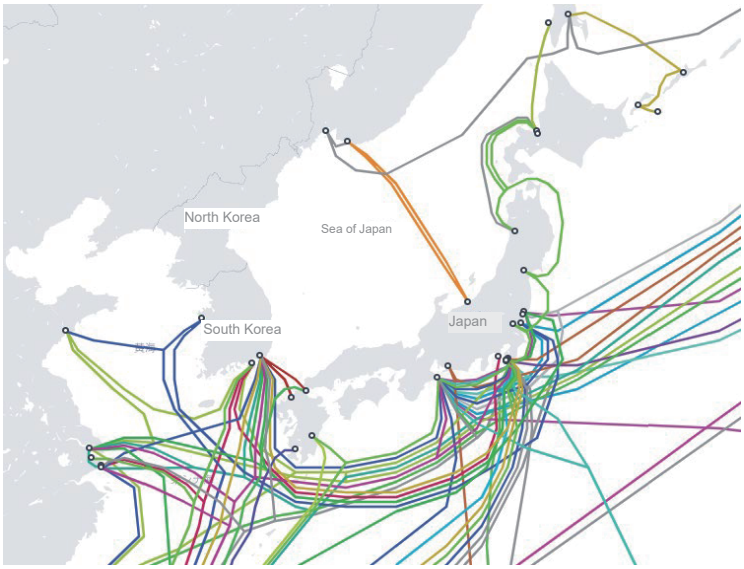
(Source) IDC Japan[10]

Moreover, as approximately 99% of international communications traffic goes through submarine cables, their importance is growing, associated with the probability of a further increase in international traffic is expected. However, Japan's submarine cable network is underdeveloped (a missing link) in areas off the Sea of Japan coast because domestic submarine cables have been laid mainly off the Pacific coast. In addition, cable landing stations, which represent the ends of submarine cables, are concentrated in the Boso Peninsula **(Figure**

[9] Rakuten Mobile previously planned to move forward, by around five years to the summer of 2021 or earlier, the achievement of the goal of raising the population coverage rate to 96% by the end of March 2026 under a base station development plan submitted to and approved by the Ministry of Internal Affairs and Communications. However, the goal was achieved only in February 2022 due to delays in the development of 4G base stations caused by a semiconductor shortage.
[10] https://www.idc.com/getdoc.jsp?containerId=prJPJ48272821

2-2-1-2). Risk, such as the disconnection of submarine cables, has materialized, as was the case when a volcanic eruption in Tonga caused disruptions to international communications due to submarine cable breakage, or when the Great East Japan Earthquake caused multiple submarine cables to be severed. Therefore, it is necessary to assume various risks, including natural disasters, human error, and sabotage, and to take steps to secure flows of communications traffic via submarine cables.

Figure 2-2-1-2 Map of submarine cables laid around Japan

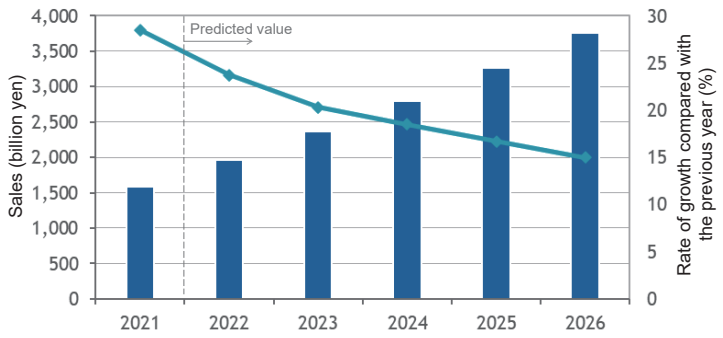


(Source) TeleGeography, "Submarine Cable Map"[11]

According to the results of observations[12] by the Network Incident Analysis Center for Tactical Emergency Response (NICTER), which is operated by the National Institute of Information and Communications Technology (NICT), the annual total number of packets observed per IP address, which represents the level of cyberattack-related internet activity, declined from the previous year (by around 6%) to approximately 1.75 million in 2021, marking a turnaround from the uptrend that had continued since 2012. However, compared with 2019, that number still represents an increase of around 40% over a two-year period, reflecting a continued flood of cyberattack-related packets. Furthermore, when it comes to data security, Japan has fallen into a vicious spiral of failure: the country depends heavily on foreign sources for its supply of cybersecurity products, services and information, resulting in a lack of access to real-world data essential for research and development, which has impeded the development of original Japanese cybersecurity technology, and this situation is in turn undermining the ability to collect and analyze cyberattack information in Japan.[13]

Although the development of cloud services has been remarkable in Japan as well (**Figure 2-2-1-3**), U.S. and other foreign vendors have come to dominate the cloud service market in Japan, raising concerns in some quarters about an excessive dependence on foreign sources.

Figure 2-2-1-3 Changes and forecasts for the market size (sales) of public cloud service in Japan



(Source) IDC Japan[14]

[11] https://www.submarinecablemap.com/
[12] NICT (2022) "NICTER Observation Report 2021," https://www.nict.go.jp/press/2022/02/10-1.html
[13] Ministry of Internal Affairs and Communications, Cybersecurity Task Force (2021), "ICT Cybersecurity Comprehensive Measures 2021" https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html
[14] https://www.idc.com/getdoc.jsp?containerId=prJPJ48986422

In May 2022, the Economic Security Promotion Act (formally known as the Act on Promotion of Economic Security through Integrated Implementation of Economic Measures), which has four pillars—securing stable supply of critical goods, ensuring stable provision of basic infrastructure services, supporting the development of key advanced technologies, and non-disclosure of patent applications—was enacted, to be enforced in phases.

The Ministry of Internal Affairs and Communications has developed a new technology strategy intended to accelerate research and development, through intensive investment by the government in order to acquire strategic indispensability and strengthen Japan's international position with respect to the development of advanced technologies in which the country has an advantage and can lead the world, such as all-photonics network technology[15], NTN (non-terrestrial network), and secure virtualized and integrated network technology.[16]

Moreover, in order to secure the strategic autonomy of and acquire strategic indispensability for the information and communications industry, which has a growing role as a strategic infrastructure industry, the ministry has developed a comprehensive strategy which lays down the development and introduction roadmap of new technologies that could become game-changers, the processes of customer- and market-oriented business expansion, the direction of initiatives related to practical application of solutions based on the integration of "monozukuri" (traditional manufacturing) expertise and digital infrastructure, and eight priority fields.[17]

2. Current state of data governance

As mentioned in the previous chapter, the economic value of data has been dramatically rising in recent years. Data is considered to be "a key source of knowledge/wisdom, value and competitive strength, and a powerful card for the solution of social issues of Japan as an advanced country with new problems."[18] Meanwhile, concerns are mounting globally over the concentration of user data, including personal preferences and behavior history, among the global platformers and how this data is analyzed and used by them as described in Chapter 1, Section 5. For example, in Japan, some media reported the case where the personal information of users held by a domestic business was accessible by a foreign corporation which had been entrusted with operations,[19] and it has been pointed out that there are growing risks due to the inappropriate handling of information by business operators sitting on a large mass of information amid the progress of globalization, including the overseas consignment of development, and the use of diverse vender products and overseas data centers.

In this context, **data governance** initiatives toward the effective and proper use of data are progressing in Japan and other countries. Under the **European Strategy for Data** released in February 2020, the **EU** is developing unified rules on access to the enormous quantity of data generated by individuals and enterprises, with the aim of constructing a single data market and promoting technological innovations so that it can hold a leading position in the digital economy.[20] The **Data Governance Act**, which was developed based on the strategy, proposes a mechanism for the use of data that suits needs across industries and borders in order to promote reliable data distribution.[21] In addition, the Proposal for a Regulation on harmonized rules on fair access to and use of data [22] that provides the right to access industrial data, etc., was published in February 2022. **The United States**, which is home to many global IT giants, including GAFA, has not made any strong interventions in the promotion of data utilization in the private sector. However, **both federal and state governments are working proactively in the public sector**. For example, the federal government is rapidly constructing a data value improvement and governance structure based on its Federal Data Strategy published in June 2019.[23] **In China, the Data Security Law** was enforced on September 1, 2021. This law clearly defined the concept of data, established basic systems including protection of data classification/grading, risk assessment, monitoring/early warning and emergency response, and clarified the obligations to be fulfilled when handling data.[24]

In line with these international trends, Japan made a cabinet decision in June 2021 on a **National Data Strategy and** compiled challenges and countermeasures with seven layers, including strategy and policy, organization, rules and service platform.[25]

MIC with cooperation of bodies concerned conducted a questionnaire survey to understand actual situations including efforts by telecommunications carriers and examined their security measures and data handling. In addition, the Act Partially Amending the Telecommunications Business Act (Act No. 70 of 2022) was enacted in June 2022. The act obligates the proper handling of user

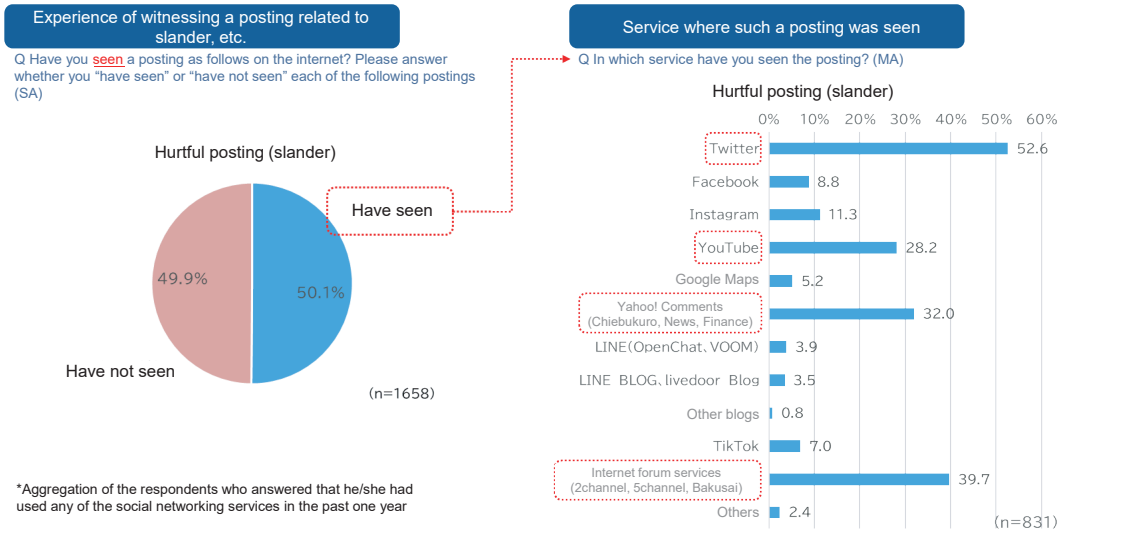
[15] One of the major technical fields under the IOWN initiative, which is being promoted by NTT.
[16] For further details, see Chapter 4, Section 7.
[17] For further details, see Chapter 4, Section 1.
[18] National Data Strategy (Cabinet Decision on June 18, 2021)
[19] Later, it was confirmed that access by the foreign corporation was a legitimate operation in the development and maintenance processes.
[20] https://www.jetro.go.jp/biznews/2022/02/225affa523fffc72.html
[21] https://www.pwc.com/jp/ja/knowledge/prmagazine/pwcs-view/202203/37-03.html
[22] https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data
[23] https://www.soumu.go.jp/main_content/000756398.pdf
[24] https://www.jetro.go.jp/ext_images/_Reports/01/580a6448fa87f0bb/20210056_04.pdf
[25] National Data Strategy (Cabinet Decision on June 18, 2021)
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/63d84bdb-0a7d-479b-8cce-565ed146f03b/02063701/policies_data_strategy_outline_02.pdf

information obtained by telecommunication carriers, which has a significant impact on the interests of users, by formulating and disclosing handling rules for such information. Moreover, when a telecommunication carrier intends to transmit a program that orders the transmission of information on a user to a third party, etc., carriers have to provide users with an opportunity to confirm, for example. Since then, the public and private sectors have been jointly advancing discussions toward the smooth enforcement of the act.

3. Response to illegal/harmful information

With the dissemination of various Internet services including social networking and video streaming services, anyone can send information, enormous quantities of information are being distributed, and a variety of information is readily available. While ICT has become an infrastructure that forms the foundation for daily life and socio-economic activities, the spread of illegal/harmful information has become a challenge, which includes the distribution of expressions slandering people and contents infringing intellectual property rights. According to a survey conducted by MIC[26], about half of the respondents (50.1%) have seen "a hurtful post (slander)" **(Figure 2-2-3-1)**.

Figure 2-2-3-1 Experience of witnessing a post related to slander, etc. and the service where such posts were found



(Source) From Material 5 of MIC Study Group on Platform Services (36th meeting)[27]

Recently, the problem of disinformation has emerged, including false information distributed with intention and information of unknown authenticity. It has also been pointed out that there are biases in the information acquired by users on platform services such as social media. For example, communities of users with similar interests and opinions are formed and the community's users see only opinions similar to theirs (echo chamber); and other information, outside of their personalized, desired information, is automatically excluded (filter bubble). This problem is emerging across the world. Various initiatives are being conducted to address this around the world, such as efforts to improve the ICT literacy of users, to promote fact checking and to mediate information distribution by business operators.

Institutional responses are also progressing. For example, in April 2022 the EU provisionally agreed on the Digital Service Act, which stipulates the responsibilities of all intermediary service providers (e.g., platformers) on the distribution of illegal contents, and obligations to protect users according to the scale of the business. In the United States, the problem of disinformation at the time of the 2016 presidential election triggered surveys and discussions on disinformation countermeasures. A public hearing on the efforts of platformers was held at Congress in a move to review Section 230 of the Communications Decency Act of 1996, which stipulates that providers are not responsible for content disseminated by a third party.

In Japan too, institutional measures have been implemented to facilitate relief for sufferers of rights violations through slander, etc., over the Internet, which includes an amendment of the Provider Liability Limitation Act to establish a new judicial procedure (for non-contentious cases) for the disclosure of sender information (the amended act was enacted in April 2021 and enforced in October 2022), and an amendment of the Penal Code to raise the statutory penalty of insults (the amended code was enacted in June 2022 and the statutory penalty of contempt is to be enforced in summer of the same year), for example. In addition, under the Policy Package for Dealing with Slander Over the Internet, which

[26] Questionnaire survey on actual state of distribution of slander on the Internet
[27] https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/02kiban18_02000207.html

was compiled and published in September 2020, MIC in collaboration with relevant groups has been implementing the following: a system to disclose the identification information of senders; user education on information ethics and ICT literacy; support for voluntary initiatives by platformers and improvement of their transparency and accountability (through the continuous monitoring of platformers); and enhancement of the consultation counter functions (strengthening the system of the Illegal/Harmful Information Hotline, strengthening of collaboration among consultation centers and dissemination of the information on multiple consultation centers). In addition, private businesses and groups are also taking actions, which include handling reports from the public regarding illegal content and harmful content on the Internet by the Safer Internet Association (SIA).

With regard to disinformation, MIC is continuously conducting surveys on the state of contact with, reception and spread of disinformation by citizens and their attitude to information distribution, and considering measures against disinformation based on the results, etc. Furthermore, diverse stakeholders in the private sector are advancing various initiatives. Examples are initiatives to promote fact checking, including the development and publication of the fact check guidelines and rating standard by the Fact Check Initiative Japan, and the study of disinformation countermeasures by the Forum against Disinformation set up by SIA.