Japan welcomes the opportunity to respond to General Assembly Resolution 73/27 on “Developments in the field of information and telecommunication in the context of international security” and Resolution 73/266 on “Advancing responsible State behavior in cyberspace in the context of international security”.

1 General appreciation of the issues of information security
Knowledge, technologies, and services in cyberspace, such as AI, IoT, Fintech, Big Data, and 5G, are becoming established in society and leading to innovations that are transforming the existing structures in our socio-economic activities and the daily lives of people, and these transformations are bringing about progress in the unification of cyberspace and real space. In order to enjoy the benefits of the knowledge, technologies, and services of cyberspace, it is essential to control the latent uncertainties always therein. When such control is not possible, the potential exists for cybersecurity-related threats to increase rapidly.

➢ Benefits of Cyberspace
The number of Internet users in the world is rising, as is the spread of the Internet itself. Furthermore, in terms of devices, the rate of personal smartphone ownership has increased significantly, and the Internet usage rate is also rising. The ratio of social media users is also rising, as a result of which an environment now exists for easily communicating in cyberspace. The increasing adoption of services in cyberspace by society has promoted not only the free flow of information, but also the formation of diverse communities and the sharing of information. There has been progress in the area of financial activities as well, including online shopping, stock trading, and online banking, while new services in the areas of Fintech and the sharing economy are appearing regularly and leading innovation. There has also been progress in the use of Information and communication technology in medicine and nursing, welfare, education and other areas related to social issues such as the declining working-age population and the aging of local communities.

➢ Increasing Threats in Cyberspace
While AI, IoT and other technologies and services have the potential to bring many benefits to people, there is always the latent risk that the providers of these technologies and services will lose the ability to control them, in which case they can cause immeasurable economic and social loss or damage. As the unification of cyberspace and real space proceeds, the likelihood of this increases exponentially. Furthermore, cyberspace is a place unrestricted by space or time where anyone, including malicious actors, can misuse and abuse new information and communication technologies with ease. The very nature of digital technology allows malicious actors to easily
copy and distribute sensitive data and information, launch attack programs, and flexibly incorporate and make free use of emerging technologies such as AI and blockchain. For that reason, the attackers have an asymmetrical advantage over the defenders, and that advantage is expected to increase particularly when the defender’s formation depends on existing policies and technological systems. Given these conditions, attacks directed at IoT, Fintech including crypt-currencies, critical infrastructure, and supply chains have occurred, causing direct financial losses and the interruption of businesses and services in addition to the usual data breach, and serving to threaten the safety and security of the sustainable development of socio-economic activities and the people’s living. There have also been massive incidents suspected to have been state-sponsored. There is also concern that the credibility of the information infrastructure may be shaken if cyberspace is controlled and managed by the government in some countries from a superior position. It is believed that as cyberspace continues to become further unified with real space, there will be increased concerns over potential attempts to target weaknesses in IoT, supply chains, and open innovation, and for unintended behavior to occur in these systems. This could seriously impact not only governmental bodies and critical infrastructure operators, but also other businesses and even individuals.

➢ Adherence to the Basic Position on Cyberspace

In order to continue to deter malicious actors’ activities and guarantee people’s safety and rights, Japan retains, as its options, political, economic, technological, legal, diplomatic, and all other viable and effective means. Japan adheres to the five principles for developing and implementing cybersecurity measures, which are: (i) assurance of the free flow of information; (ii) the rule of law; (iii) openness; (iv) autonomy; and (v) collaboration among multi-stakeholders.

(i) Assurance of the Free Flow of Information

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

(ii) The Rule of Law

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

(iii) Openness
To achieve the sustainable development of cyberspace as a space to generate new values, cyberspace must be open to all actors without restricting the possibilities of linking diverse ideas and knowledge. Japan adheres to the position that cyberspace must not be exclusively dominated by a small group of actors therein.

(iv) Autonomy

Cyberspace has developed through the autonomous initiatives of multi-stakeholders. It is inappropriate and impossible for a state to take on the entire role of maintaining order for cyberspace to sustainably develop as a space where order and creativity coexist. The only approach to maintain order and deter and address the behavior of malicious actors is for various social systems to function autonomously. Japan will promote this approach.

(v) Collaboration among Multi-stakeholders

Cyberspace is a multi-dimensional world established through the activities of multi-stakeholders, including the state, local governments, critical infrastructure operators, cyber-related and other businesses, education and research institutions, and individuals. For the sustainable development of cyberspace, all actors are required to consciously fulfill their respective roles and responsibilities. This will require coordination and collaboration in addition to individual efforts. States have the leading role in promoting this coordination and collaboration, and will promote measures enabling the fulfillment of such roles.

2 Efforts taken at the national level to strengthen information security and promote international cooperation in the field

Efforts taken at the national level to strengthen information security

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

The unification of cyberspace and real space significantly increases the potential for affording abundance to society. At the same time, it also increases the opportunities for malicious actors to abuse cyberspace. The risk of economic and social loss or damage in real space is expected to
expand and accelerate exponentially. Under these circumstances, the security of cyberspace, which serves as the foundation of economic society, must be ensured, and at the same time, its autonomously sustained evolution and development has to be ensured in order to achieve sustainable progress and wealth to society.

Recently, there has been a trend for certain nations to respond to cyber threats by emphasizing management and control by the state from a dominant position. However, the strengthening of management and control of cyberspace by the state has the effect of hindering the possibility of autonomous and sustainable development. Thus, the cyberspace of today that developed through the autonomous initiatives of all stakeholders must be respected, and cybersecurity must be secured through collaborative and cooperative initiatives with those stakeholders. Based on this understanding, mindful of the state of affairs to be pursued for 2020 and beyond and taking into consideration the hosting of such international events as the Games of the XXXII Olympiad and the Tokyo 2020 Paralympic Games (hereinafter referred to as “the Tokyo 2020 Games”), Japan will spare no efforts regarding cybersecurity measures by clarifying the basic vision of cybersecurity, identifying new issues that need to be tackled; and swiftly implementing measures.

➢ Efforts taken at the national level to promote international cooperation

Because the effects of incidents in cyberspace can easily extend beyond national borders, cyber incidents overseas can always affect Japan. Japan will cooperate and collaborate with governments and the private sector worldwide to ensure the security of cyberspace and work towards both the peace and stability of the international community and the national security of Japan. To this end, the government will proactively contribute to various international discussions and work for the sharing of information and the development of a common understanding regarding cyber-related issues. The government will also share expertise with foreign countries, promote specific cooperation and collaboration, and take action.

With regard to Sharing Expertise and Coordination Policy, the government will work through bilateral dialogues and international conferences on cybersecurity to exchange information on cybersecurity policies, strategies and system to respond, and utilize that knowledge in planning Japan’s cybersecurity policy. We will also strengthen our cooperation and collaboration regarding cybersecurity policy with strategic partners that share basic principles on cybersecurity with us.

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

In the light of the diplomatic aspects of cyber-related international cooperation, our commitments are consisted of three pillars: “Rule of law”, “Confidence Building Measures”, and
“Capacity-building” in cyberspace.

- The promotion of the rule of law is important for international peace and stability and Japan’s national security. Japan’s position is that existing international law, including the United Nations Charter, applies to cyberspace also, and Japan will proactively contribute to discussions on the individual and specific applications of existing international law and the development and universalization of norms. With regard to measures against cybercrime, the National Police Agency and other relevant ministries and agencies will collaborate to further promote international partnerships through international investigative cooperation and information sharing with international organizations, law enforcement agencies and security information agencies in foreign countries leveraging frameworks such as the Convention on Cybercrime, mutual legal assistance treaties, and the ICPO.

- Japan will work to build confidence among states in order to prevent the occurrence of unforeseen circumstances and deterioration of the situation caused by cyberattacks. Due to the anonymity and secrecy of cyberattacks, there are risks that cyberattacks could unintentionally increase tensions among states and worsen the situation. To prevent such accidental and unnecessary confrontations, it is important to build up international communication channels during peaceful times in preparation for the occurrence of incidents that extend beyond national borders. It is also necessary to increase transparency and build confidence between states through the proactive information exchange and policy dialogues in bilateral and multilateral consultations. The government will also cooperate with other states to consider a mechanism for coordinating issues regarding cyberspace. In this context, Japan eagerly promotes confidence building measures (CBMs) including by initiating the establishment of and co-chairing ASEAN Regional Forum Intersessional Meeting in the field of cybersecurity, while steadily implements capacity-building assistance mainly in the Asia-Pacific region.

- With regard to capacity-building, as interdependence across borders has deepened, it is not possible for Japan to secure peace and stability alone. Global coordination to reduce and eliminate cybersecurity vulnerabilities is essential to ensuring Japan’s national security. From this standpoint, assisting capacity-building in other states ensures the stability of the lives of Japanese residents and the activities of Japanese companies in other countries that depend on critical infrastructure in those states as well as the sound development of the use of cyberspace there. At the same time, it is also directly connected to ensuring the security of all cyberspace and contributes to the improvement of the security environment for the entire world including Japan. Also, in the field of cybercrime, Japan is one of the few Non-European Parties to the Convention on Cybercrime and takes a positive role in promoting the convention, which is an important legal framework for countering cybercrime, through capacity-building assistance in the Asian region.
3 Relevant international concepts aimed at strengthening the security of global information and telecommunications system

Japan supports consensus agreements of the previous UN GGEs that existing international law applies in cyberspace. We have seen the discussion on the development of normative behavior, the operationalization of CBMs, and capacity-building as the key approaches to shaping responsible state behavior in cyberspace. In particular, Japan recognizes that implementation of non-binding and voluntary norms of responsible state behavior in cyberspace, as referred to in the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications Technology (ICT) environment (GGE), must be the foundation for ensuring international stability and predictability, and for future discussions on this issue. In this regard, we believe any attempts to conclude newly comprehensive treaties or similar instruments would not positively enhance cybersecurity at present.

4 Possible measures that could be taken by the international community to strengthen information security at the global level

Japan, as a responsible state, while promoting coordination with relevant regional frameworks by the international community based on existing international law, and all concepts identified through the GGE, believes that developing a common understanding of the voluntary and non-binding norms of the responsible state behavior, and the implementation of these norms, will contribute to the strengthening of international security.

5 The content of the concepts mentioned in the reports of the Group of Governmental Experts

Japan believes that it is effective and meaningful for all states to take into consideration the following concepts identified by the GGE

➢ Influence on the international community by malicious cyber acts

To flexibly incorporate the rapid development of information and communications technologies in our lives, and to prevent the damage stemming from malicious cyber acts, we should acknowledge the importance of foreseeing existing and potential threats in cyberspace and how the international community could be affected by them.

➢ Implementation of voluntary, non-binding norms of the responsible state behavior

To minimize the effects of malicious cyber acts and to deter those who would commit them, we should recall the significance of the consensus GGE report, including the voluntary and non-binding norms of responsible state behavior referenced therein. We should deepen our discussions, in collaboration with relevant regional organizations, to make practical and effective use of these worthwhile efforts.
Promoting the implementation of voluntary, non-binding norms of the responsible state behavior and the cooperation for relevant confidence-building measures and capacity-building

To further enhance each state’s effort to develop and maintain a free, fair, and secure cyberspace in the context of international security, we should reaffirm that all nations have strong will to eliminate security holes in cyberspace and prevent cybercrime and other malicious acts. In this context, the group member should dedicate consistently to evoke all states into their steady implementation of the voluntary, non-binding norms of the responsible state behavior, including CBMs and cooperation to help build national capability to implement the above-mentioned voluntary, non-binding norms and recommendations, including through the process of the next GGE and Open-Ended Working Group. (end)