(Provisional Translation)

Basic Policy on Cybersecurity Capacity Building Support for Developing Countries

December 14, 2021
Approved by the Cybersecurity Strategic Headquarters

1 Basic Understanding

(1) With regard to capacity building in the cybersecurity field, the National Security Strategy (approved by the Cabinet in December, 2013) states, “With regard to cyberspace, based on the recognition of ensuring the free flow of information in cyberspace, Japan will actively cooperate with like-minded countries in the development of international rules on the premise that existing international law applies to cyberspace. Japan will also vigorously support the capacity building efforts of developing countries in this area.” The Development Cooperation Charter (approved by the Cabinet in February, 2015) lists enhancing the capacity of developing countries in relation to cyberspace as a measure for “sharing universal values and realizing a peaceful and secure society,” which is a priority issue in development cooperation. The Basic Policy for Reforms toward the Realization of Digital Society (approved by the Cabinet in December 2020) sets “forth enhancement of security through cybersecurity measures” as a basic principle for creating a digital society and countries that Japan will actively conduct international cooperation and contribution.

And the “G7 Principles and Actions on Cyber” issued by the G7 in May 2016 during the Ise-Shima Summit confirmed that G7 leaders will endeavor to strengthen our cooperation on “capacity building to promote security and stability in cyberspace. Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security adopted by the United Nations Open-ended Working Group (OEWG) on Cybersecurity in March, 2021 recommends on “Further promotion of coordination and resourcing of capacity-building efforts”, and Report of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security adopted by the United Nations Group of Governmental Experts (GGE) on Cybersecurity in July, 2021 also identified necessity of “Further strengthening international cooperation and capacity-building in order to ensure all States can contribute to the maintenance of international peace and security”.

Furthermore, the Cybersecurity Strategy 2021 (approved by the Cabinet in September, 2021) identified necessity of further enhancing international cooperation and collaboration as the digital economy has spread and ensuring "a free, fair and secure cyberspace" becomes more important than ever, and it stated with regard to capacity building support, “Other countries are providing various capacity building supports for developing countries. Under Japan’s basic principles, Japan will provide the required supports strategically and efficiently as a nationwide effort, and also in a multi-layered manner in collaboration with diverse stakeholders including like-minded countries, international organizations such as the World Bank, industry and academia.”.

(2) Such support is important for Japan from the following perspectives.

(i) Reducing international cybersecurity vulnerabilities and risks for Japan and the rest of the world.

(ii) Ensuring the stability of the lives of Japanese residents and the activities of Japanese companies that depend on critical infrastructure in recipient countries.

(iii) Obtaining general understanding of Japan’s position based on the basic principles of assurance of the free flow of information and the rule of law among those countries.

(iv) Developing a foundation for Japan’s information and telecommunications industry and others to operate locally in those countries.

(v) Contributing to the reinforcement of government policies such as the Infrastructure Export

Strategy and Free and Open Indo-Pacific.

(3) Cybersecurity capacity building support in developing countries have been conducted by many ministries. However, amid tight fiscal conditions, it is becoming increasingly important to provide support strategically and efficiently as a nationwide effort, and to engage in close collaboration between the public and private sectors, as well as between relevant ministries, in order to maximize the benefits of the support.

With European countries and US increased attention to the Indo-Pacific region, the COVID-19 pandemic has led to growing opportunities for countries to provide the region with capacity building online, whether it is from the public or private sector. As such, it is crucial for Japan to leverage the rapid spread of remote work environments as an opportunity to take the necessary steps. We should build an environment that allows various experts in the public and private sectors to flexibly support capacity building from anywhere, and also a framework that enables effective support, according to the diverse needs of developing countries, in collaboration with diverse stakeholders including like-minded countries, international organizations such as the World Bank, industry and academia.

2 Approaches of Support

Capacity building support in the cybersecurity field is largely categorized into four groups: (1) support for ensuring cyber hygiene through the protection of critical infrastructure and other means, (2) support for measures against cybercrimes, (3) sharing understanding and cyber situational awareness of international rules and confidence building measures, and (4) human resources development and other cross-sectoral areas. However, the status of systems and readiness in the cybersecurity field differs among developing countries to be supported, so it is necessary to identify new threats in cyberspace and the needs of each country, and to provide support in a way that makes the most of Japan's strengths. To ensure efficient and effective support, these initiatives must be carried out by continuing to exchange information and coordinate policies to the extent possible with like-minded countries, including in particular the United States, Japan's ally. This will not only help avoid redundant support, but also enable the pursuit of synergy effects.

(1) Support for ensuring cyber hygiene through the protection of critical infrastructure and other means

Capacity building support in the cybersecurity field has been provided mainly for government agencies in ASEAN member states to date. While continuing to support government agencies, we will enhance support for critical infrastructure, an area where there are growing needs for supporting measures as infrastructure development advances in each country based on the relationship so far. In addition, we will expand the scope of support in the Indo-Pacific region based on past achievements and experiences in capacity building support in the ASEAN region.

(a) ASEAN region

For the government agencies of ASEAN member states, we have built a positive relationship of trust through continuous support in collaboration with like-minded countries for over a decade. We have undertaken initiatives including the ASEAN-Japan Cybersecurity Policy Meeting, the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), and the Industrial Cyber Security Center of Excellence (ICSCoE) implemented by Information-technology Promotion Agency, Japan (IPA). In particular, we have been putting greater emphasis on AJCCBC, for example, by providing online exercises and expanding training options targeted to government officials and employees of critical infrastructure operators in ASEAN member states. Furthermore, the Ministry of Economy, Trade and Industry (METI) and ICSCoE are conducting industrial control system

cybersecurity exercises for the Indo-Pacific region, including ASEAN member states, in cooperation with the United States and Europe, in order to improve the cybersecurity capability for entire supply chain in the Indo-Pacific region and strengthen cooperation with each country.

In addition, the Japan International Cooperation Agency (JICA) has launched country-specific support in Indonesia, Vietnam, and elsewhere to address unique issues and challenges faced by each country. In particular, the technical cooperation project started in 2019 in Indonesia is being conducted as an industry-government-academia effort beyond an intergovernmental framework to advance capacity building support. In this project, JICA teams up with local universities to support human resources development for critical infrastructure operators.

In recent years, infrastructure development and digitalization have been advancing among ASEAN member states, driven by growing economies and government capabilities. As a result, support for measures targeting the critical infrastructure field that includes the private sector is becoming increasingly important. Moreover, gaps in cybersecurity capabilities have been widening among countries in the region.

Given these circumstances, it is vital going forward to enhance support for measures targeting the critical infrastructure field, etc. through public-private collaboration including Japanese businesses with strengths in infrastructure, etc., and to reinforce training for companies of the target country, with respect to countries with relatively advanced capabilities.

The role required of the Japanese government in this effort is to cooperate with the governments of each country, and to promote initiatives pursued by private businesses in a way that supports local cybersecurity policies. In order to advance continuous measures through private activities, it is necessary to ensure that the support is devised in alignment with the free management decision of private businesses. Moreover, in order to advance such initiatives effectively, it is necessary to understand the cybersecurity needs of ASEAN and other regions, and to arrange a framework that enables optimal measures to be provided making full use of Japan's resources.

As for countries and regions with relatively more room for capacity building, it is necessary to continue to provide support for government agencies, using framework such as Mekong-Japan cooperation and BIMP-EAGA+Japan, while collaborating with relatively advanced countries in the ASEAN region and like-minded countries outside the region. Taking this into account, we will enhance future activities related to AJCCBC by collaborating with like-minded countries and other third parties. In addition, we will move forward to further increase training options to enable ASEAN member states to independently conduct exercises, and to diversify our activities in light of local demands. At the same time, while there are increasing numbers of support frameworks targeting the ASEAN region as a whole by European countries and US, the need for country-specific support tailored to each country's capabilities, such as the kind provided by JICA, is growing, so we will continue to enhance support accordingly.

(b) Regions other than ASEAN

Based on the experience we have cultivated to date through support for ASEAN member states and interstate relations with the region, we will enhance support in regions other than ASEAN, with a focus on the Indo-Pacific region (Asia, Oceania, etc.).

For the meantime, for example, we will continue to carry out the industrial control systems cyber security exercises for the Indo-Pacific region in cooperation with the United States and Europe provided by METI and ICSCoE, as well as implementing country-specific support tailored to each country's capabilities, such as the kind provided by JICA.

In selecting the countries to be supported, we will take various factors into consideration, including the status of activities of Japanese businesses, geographic importance in terms of telecommunication network nodes, and status of support by like-minded countries and international organizations, and focus on countries where we can expect the greatest results with a limited budget. We will also consider the possibility of support in Africa.

(2) Support for measures against cybercrimes

We are faced with a need to enhance capabilities to respond to and investigate crimes such as stealing personal and corporate information and intellectual properties, and hacking into the systems of government agencies and businesses that provide a foundation indispensable to our daily lives and economic activities, while deterring as many crimes as possible, and ensuring a free, fair and secure cyberspace based on the rule of law. To do so, collaboration (especially between law enforcement agencies) with the international community including developing countries is essential. We must continue to actively engage in this effort using frameworks such as Cybercrime Dialogue and relevant meetings held by Parties to the Convention on Cybercrime, in addition to providing more specific support. This specific support includes training on developing legislation related to measures against cybercrimes and criminal investigation methods, funding the United Nations Office on Drugs and Crime (UNODC)'s Global Programme on Cybercrime, and providing training related to criminal justice in collaboration with the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) and others.

(3) Sharing understanding and cyber situational awareness of international rules and confidence building measures

Japan takes the position that the existing international law applies to cyberspace as well. As it is necessary to lead to formulating international rules and norms in cyberspace by participating in discussions on specific application of international law and other measures, we will enhance capacity building support efforts for each country on application of international law and the norms.

Moreover, it is necessary to establish international communication channels from normal times to build confidence, while sharing understanding with other countries and to mutually raise awareness on matters in order to prevent the occurrence of unforeseen circumstances caused by cyberattacks.

Therefore, we will continue such initiatives as awareness raising activities on cybersecurity (e.g., joint creation of awareness-raising content with ASEAN, opportunities for foreign students to exchange opinions), and bilateral and multilateral workshops and cyber talks. At the same time, we will also actively work to create international rules and share understanding with other countries, using forums for multilateral talks, such as the UN GGE and OEWG, and the ASEAN Regional Forum (ARF) Inter-Sessional Meeting on ICTs Security.

We will also secure capabilities for acting responsible State behavior in cyberspace, through efforts by multi-stakeholders including private companies, academia, and technical communities.

(4) Human resources development and other cross-sectoral areas

To date, relevant ministries have collaborated to provide human resources development programs according to the needs for support identified by the respective government agencies of other countries in the respective fields. Going forward, we will be required to meet requirements for digital transformation (DX), address growing needs for support in the critical infrastructure and other fields, and provide support even more efficiently with a limited budget. To those ends, we will discuss how to move forward while collaborating even more closely between relevant ministries, such as standardizing the basic skillsets of human resources in each field.

Moreover, based on the global lack of advanced experts in the cybersecurity field has presented a major challenge for Japanese businesses operating in the ASEAN region in terms of securing the necessary human resources, we will develop human resources to support the activities of Japanese businesses overseas, including ASEAN, over the medium to long term, and create an environment that facilitates understanding of diverse cultures and acceptance of foreign resources at Japanese businesses through industry-government-academia collaboration.

Under this basic policy, the Cabinet Secretariat will lead nationwide efforts based on close collaboration between relevant ministries and the public and private sectors, using various policy means, and actively support developing counties in building capacity in the cybersecurity field.

(End)