JICA Global Agenda for

No. 15 Digital for Development

Cluster Strategy for Cybersecurity

Japan International Cooperation Agency (JICA) works toward the achievement of the Sustainable Development Goals (SDGs).

2023.05

1. Purpose

While the benefits of the digital socio-economy have expanded in recent years, developing countries also face serious cybersecurity risks, such as ransomware threats, cyber-attacks against critical infrastructure (e.g., energy, finance, telecommunications, health), leakage of confidential information through supply chains, social disruption through disinformation, and personal data breaches.

This cluster strategy aims to **achieve a society capable of responding increasingly serious threats in cyberspace and protecting people's lives and dignity (Cybersecurity for All)**, and to promote cooperation to enhance the cybersecurity resilience of developing countries, particularly in the Indo-Pacific region.

The use of appropriate digital technologies to achieve the SDGs is expected, and the cybersecurity is important as a safeguard to respond to the negative aspects that may arise in the process of digitalization. (Related SDGs: 4. Quality Education, 5. Gender Equality, 7. Affordable and Clean Energy, 8. Decent Work and Economic Growth, 9. Industry, Innovation and Infrastructure, 11. Sustainable Cities and Communities, 16. Peace, Justice and Strong Institutions, 17. Partnerships for the Goals)

2. Current Situation and Development Approaches

As digital technologies permeate people's lives and industrial activities, and as the benefits of a digital socio-economy grow, so do the threats posed by cyber-attacks. Even in developing countries, cyber-attacks have led to disruptions in critical infrastructure services that support people's daily lives, such as power outages, disruption in healthcare services, fraudulent central bank transfers, loss of citizen information, online phishing, and other cybersecurity-related harm at the individual level. Cyber risks are increasing as developing countries go digital.

Starting in 2019, the Government of Japan began advocating "Data Free Flow with Trust (DFFT)" to promote the international flow of data that is useful for solving business and social challenges, while ensuring trust in privacy and intellectual property rights. In addition, the Government of Japan formulated the "Basic Policy on Cybersecurity Capacity Building Support for Developing Countries" (2021) to promote

international cooperation in the areas of securing cyber hygiene for critical infrastructure protection, cybercrime prevention, international rule making, trust building measures, and human resource development in order to reduce international cybersecurity risks with a focus on the Indo-Pacific region based on experiences in capacity building support in the ASEAN region. And the QUAD Joint Leaders' Statement (2022) committed that Japan, the United States, Australia, and India would coordinate capacity building programs in the Indo-Pacific region with regard to cybersecurity.

Governments in developing countries are also working to strengthen their cybersecurity systems, but the situation is not satisfactory in the majority of countries. Reasons for this include a lack of understanding of cybersecurity throughout the country and the difficulty of continuously strengthening systems and building capacity to deal with the ever-changing and diverse threats in cyberspace.

3. Development Scenario and Key Concepts

A 100% secure cyberspace does not exist. In order for each country to respond autonomously to the ever-changing cyber threats, it is necessary to improve resilience by balancing and strengthening the following five perspectives: **(1) Legal** (establishing responsible organizations, developing legal systems for personal information protection and measures against illegal acts, etc.), **(2) Organization and Strategy** (developing national strategies and promotion structures), **(3) Technical** (improving risk handling capabilities), **(4) Capacity building** (developing public and private sector human resource development and promotion/awareness activities structures), and **(5) Cooperation** (cooperating with domestic, foreign, and international organizations).

Based on JICA's past experiences with supported countries, and referring to the Global Cybersecurity Index (GCI) published once every few years by the International Telecommunication Union (ITU), the following four stages are hypothesized to improve the cybersecurity response capacity of developing countries.

1) Initial Stage

A dedicated cybersecurity agency does not exist, or its staff and budget are limited. Cybersecurity response capabilities are extremely limited, and cyber-attacks and damage are not detected when they occur.

2) Growing Stage

Cybersecurity response capabilities of core central government agencies are being improved. While awareness within the central government has generally improved, national CSIRTs (Computer Security Incident Response Teams) have improved their security response capabilities, and limited awareness and personnel training activities have been conducted, cybersecurity measures for critical infrastructure have not progressed and risks remain high.

3) Networking Stage

In addition to central government agencies, cybersecurity measures are being broadened and deepened in critical infrastructure (private enterprises) and other public organizations. Collaboration among government agencies and between the public and private sectors will also be deepened, and activities will be carried out to strengthen overall security through inter-organizational cooperation with neighboring countries.

4) Self-sustaining Stage

A mature stage with increased cybersecurity resilience in which widespread social structures are in place to protect those connected to cyberspace. A virtuous cycle is formed, in which the activities necessary to secure the digital economy of the country and region are self-sustaining.

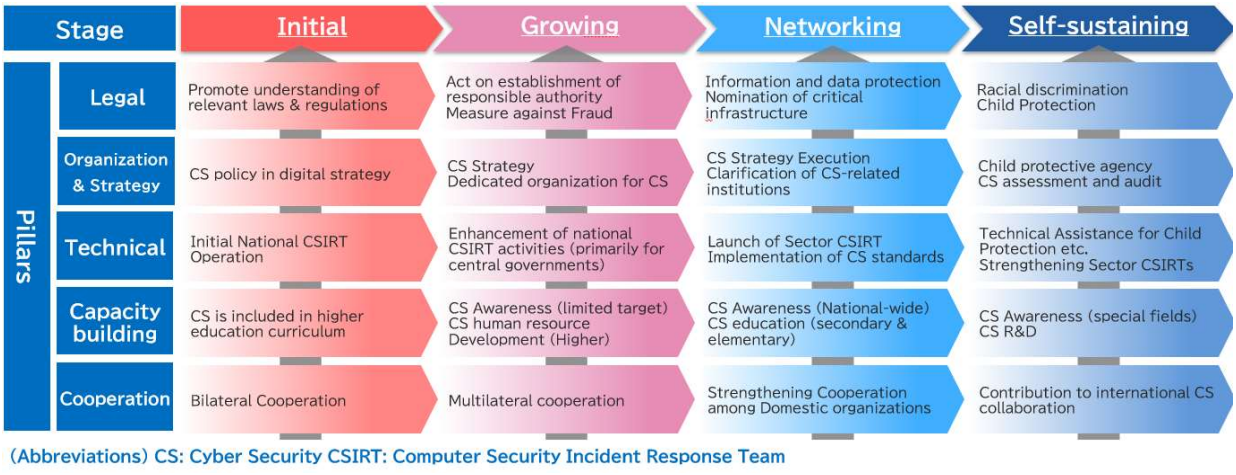

Figure1) Key actions at each stage

4. Implementation Direction

In light of the Japanese government's vison on a "Free and Open Indo-Pacific" (FOIP), JICA’s initial focus countries will be in the regions of Southeast Asia and South Asia, where economic ties with Japan are particularly strong. Meanwhile, possible cooperation in Oceania, Africa, Central and South America, etc. will also be considered upon request, taking into account the needs of each country as well as the systems and activities of other countries and international organizations in these areas.

JICA's areas of cooperation will be determined based on the actual situation of the partner country. In bilateral cooperation, JICA will mainly focus on technical cooperation in the areas of increasing "Technical " and "Capacity building", and when it is confirmed that appropriate systems are in place and operational resource allocation is secured in the partner country, financial cooperation (facilities and equipment) that contributes to this area will be considered.

To achieve collective impact, JICA will promote its projects by (1) cooperating with relevant organizations in Japan, (2) collaborating with multilateral development partners and like-minded countries, and (3) collaborating with leading developing countries.

5. Goal, Targets, and Indicators

【Cluster-wide Goal/Targets and Indicator】: Subject of performance evaluation

Goal/Targets and Indicators	**(1) Final Goal** Build a secure cyberspace where each country can ensure free and trusted data flow. This goal is set as the digitalization of socio-economic activities will result in a significant impact on people's lives. At the same time, JICA will work with the international community to achieve a secure cyberspace in the region, with a focus on the Indo-Pacific region.[1] 1. Achieving the "Self-sustaining Stage": Southeast Asian countries at the forefront of cybersecurity 2. Reaching the "Networking Stage": Countries in Southeast Asia that are lagging behind in cybersecurity, and cooperating countries in South Asia, East and Central Asia 3. Reaching the "Growing Stage": the "Initial Stage" cooperating countries
	(2) Indirect Target Increase in the level of cybersecurity preparedness in each country Indicator 1: Improve GCI scores for the capability elements targeted for cooperation in 15 countries by FY2026. Indicator 2: Improve assessment of cybersecurity capabilities in target countries (qualitative assessment)
	(3) Direct Target 1. Capacity improvement in target perspective Indicator: Improve the target capability elements based on the local scenario of the target country (quantitative and qualitative assessment). The local scenario is determined for each project. 2. Expansion of the JICA cybersecurity cooperation network Indicator: More than 30 countries will participate in cooperation projects by FY2026, and more than 50 countries will participate.

[1] * The target countries for (1), (2), and (3) below will be determined based on the future target countries for cooperation.