50th Year of ASEAN-Japan Friendship and Cooperation

ASEAN-Japan Cybersecurity Past and Future

ASEAN-Japan

Performance Report on Cybersecurity Cooperation

IC-AJCC 2023

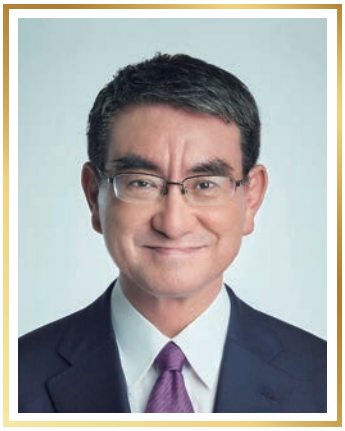
International Conference on ASEAN-JAPAN Cybersecurity Community

50th Year of ASEAN-Japan Friendship and Cooperation

ASEAN · JAPAN Cybersecurity Cooperation

NISC

Message from the Minister



Tarō Kono

(As of September 13, 2023)
Minister of Digital, in charge of Digital Administrative and Financial Reform, in charge of Digital Garden City National Plan, Minister in charge of Administrative Reform, Minister in charge of Civil Service Reform, Minister of State (Regulatory Reforms)

I would like to express my gratitude for your continuous efforts for Japan-ASEAN friendship and cooperation.

The year 2023 marks the 50th anniversary of the friendship and cooperation between Japan and ASEAN. In commemoration of this, the government held the commemorative event Japan-ASEAN Joint Forum on Cyber Security at Meiji Memorial Hall on October 5 and 6, 2023.

For half a century since 1973, Japan-ASEAN relations have made remarkable progress, building a close cooperative relationship for the peace, stability, development, and prosperity of the Asia-Pacific region.

In the current digital era, cybersecurity threats are becoming increasingly sophisticated and widespread. Governments, organizations, and individuals face a wide range of cyber risks, including hacking, data leakage, and ransomware attacks.

In order to ensure the safe and stable use of cyberspace, particularly the security of the State and critical infrastructure, it is necessary to improve response capabilities in the area of cybersecurity. For this reason, it is extremely important to promote various forms of cooperation and collaboration between ASEAN member states and Japan, including information sharing and capacity building.

The Government of Japan will continue to cooperate with the ASEAN countries to ensure a “free, fair, and secure cyberspace” and contribute to the peace and stability of the international community. Your cooperation will be greatly appreciated.

I expect that international cooperation activities between Japan and ASEAN member states will further advance through the “Japan-ASEAN Joint Forum on Cybersecurity.”

Messages from Distinguished Contributors

Expert Supervisory Policy and
Standard Center Electronic Transactions
Development Agency

Thongchai Sangsiri

Cybersecurity cooperation between ASEAN and Japan plays a vital role in enhancing the cybersecurity resilience of ASEAN member states and promoting a secure digital environment in the region. A joint statement on the establishment of the ASEAN-Japan Comprehensive Strategic Partnership in September 2023 will further strengthen the partnership.

Head of BruCERT and CWC, Cyber Security Brunei

Haji Mas Zuraime Haji Abdul Hamid

I'm truly honored to receive this prestigious award, recognizing our joint efforts in ASEAN-Japan cybersecurity cooperation. This achievement would not have been possible without the dedication and commitment from all the members of the ASEAN-Japan collaborative and the invaluable support from the Japanese government. I look forward to securing our digital future together.

Co-Founder and Chairman of
IdCARE - Indonesia Cyber Awareness and
Resilience Center of University of Indonesia.

Muhammad Salman

Thank you and highly appreciate to Japan for its continues support to ASEAN cybersecurity communities in strengthening partnership in the area of cyber security capacity building, knowledge sharing and other initiative of collaborations. Hope we could continue to hand-in-hand together to create a secure, clean and reliable cyberspace under ASEAN-Japan Cooperation platform.

Fellow,Visiting Professor,Musashino Institute for
Global Affairs,Musashino University/Advisor,
Graduate School of Public Policy,The University of Tokyo

Ryozo Hayashi

This policy meeting began in 2009. Since then, many people contributed to the development of this meeting. I would like you to remind of the special contribution made by Mr. Suguru Yamaguchi who was a professor of Nara Institute of Science and Technology, and the first Special Advisor for Information Security. He enthusiastically advocated the establishment of this meeting for the integrity of regional internet community. He also visited many countries including Asia and Africa to help establish national CSIRTs. He passed away in the middle of these activities and cannot attend todays' meeting.

ASEAN-Japan Cyber Security Policy Council Milestones

2009-2023

◆ ASEAN-Japan Information Security Policy Council established

2009

〈February〉
The 1st Information Security Policy Conference (Tokyo)
〈October〉
The 1st workshop (Tokyo)


The 1st Policy Conference

2010

〈March〉
The 2nd Information Security Policy Conference (Bangkok)
〈October〉
The 2nd workshop (Hanoi)


The 2nd Policy Conference

2011

〈March〉
The 3rd Information Security Policy Conference (Tokyo)
〈November〉
The 4th Information Security Policy Conference (Kuala Lumpur)


The 3rd Policy Conference

◆ Joint awareness raising started

2012

〈October〉
The 5th Information Security Policy Conference (Tokyo)


The 5th Policy Conference

2013

〈September〉
Cyber Security Ministerial Policy Meeting (Tokyo)
〈October〉
The 6th Information Security Policy Conference (Manila)


The 6th Policy Conference

2014

〈October〉
The 7th Information Security Policy Conference (Tokyo)


The 7th Policy Conference

2015

〈October〉
The 8th Information Security Policy Conference (Jakarta)


The 8th Policy Conference

2016

〈October〉
The 9th Information Security Policy Conference (Tokyo)

Remote Cyber Exercise and Tabletop Exercise (Exercises between ASEAN and Japan to strengthen cyber cooperation)

2017

〈October〉
Renamed ASEAN-Japan Cyber Security Policy Council

〈October〉
The 10th ASEAN-Japan Cyber Security Policy Council (Singapore)


The 10th Policy Conference

2018

〈October〉
The 11th ASEAN-Japan Cyber Security Policy Council (Tokyo)

Initiated mutual notification program activities

2019

〈October〉
The 12th ASEAN-Japan Cyber Security Policy Council (Bangkok)

2020

〈November〉
The 13th ASEAN-Japan Cyber Security Policy Council (online)

Created infographics and e-booklets in each country on the theme of "Cyber Security in Mobile Devices".

◆ Awareness campaign in each country

2021

〈October〉
The 14th ASEAN-Japan Cyber Security Policy Council (online)

2022

〈October〉
The 15th ASEAN-Japan Cyber Security Policy Council (Tokyo)


The 15th Policy Meeting

2023

International Conference on ASEAN-JAPAN Cybersecurity Community (Tokyo) IC-AJCC 2023


IC-AJCC 2023

Launched GLOBIS Graduate University "MBA for Cybersecurity" courses for examples of Industry-Government-Academia Collaboration

Examples of ASEAN-Japan Cyber Security Cooperation Initiatives

International Conference on ASEAN-Japan Cybersecurity Community

The "International Conference on ASEAN-JAPAN Cybersecurity Community" was held at the Meiji Kinenkan from Thursday, October 5 to Friday, October 6, 2023, to commemorate the 50th anniversary of Japan-ASEAN Friendship and Cooperation and to strengthen international cooperation and initiatives between Japan and ASEAN countries in the cybersecurity field. National Center of Incident Readiness and Strategy for Cybersecurity will continue to strengthen the cooperative relationship between ASEAN and Japan in cooperation with relevant ministries and agencies.

Remarks by Minister Kono


MoU Signing

Commendation for Meritorious Service


Group Photo

Joint Awareness - Raising


NISC Official Character "Secu-chan"

Started in 2012.
In 2021, created an infographic and e-booklet in each country on the theme of "Cyber Security in Mobile Devices". (Lead countries: Brunei and Singapore) In 2022, each country used them for raise awareness. (It was also published in the Cyber Policy Portal of UNIDIR (United Nations Institute for Disarmament Research).


front cover


Brunei Darussalam


Cambodia


Indonesia

Japan


Lao P.D.R.


Malaysia

Myanmar


Philippines


Singapore


Thailand


Viet Nam

RCX：Remote Cyber Exercise

Conducted online exercises every June. Created a pseudo-incident handling scenario and shared information with the CERT structure in each country by using online chat (Mattermost). The training simulated a series of incident handling activities, including incident detection, information deployment, analysis, and response, using recent cyberattacks such as ransomware as examples.

TTX：Table Top Exercise

Conducted in-person every August (cancelled in 2020; conducted online in 2021) Discussed and shared knowledge on sensitive cybersecurity issues with policymakers from different countries. Themes such as DX with Cybersecurity and Cyberattacks were selected to share information on the status of government initiatives in each country and to help policy-making.

CIIP Workshop

Activities started in 2015.
Workshops were held to share the status of activities and the latest findings from each country on Critical Information Infrastructure Protection (CIIP).

JICA Initiatives

Support for Strengthening Cybersecurity Capabilities

Signing of the minutes of the discussion on technical cooperation projects for Cambodia.

The Japan International Cooperation Agency (JICA) signed the minutes of discussion (Record of Discussions : R/D) on the technical cooperation project "Cyber Security Capacity Building Project" with the Royal Government of Cambodia in the capital city of Phnom Penh on November 29.

In Cambodia, CamCERT (Cambodia Computer Emergency Response Team), a national CSIRT (see note), is located at the ICT Security Department of the Ministry of Posts and Telecommunications. This project aims to strengthen the cybersecurity resilience of the digital society in Cambodia as a whole in the future by supporting the improvement of cybersecurity capabilities, mainly through the ICT Security Department, to respond to cyber-attacks that are becoming more sophisticated every day.

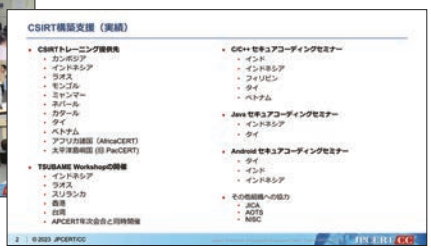
Through this project, we will contribute to SDGs (Sustainable Development Goals) Goals 9 (Create a foundation for industrial and technological innovation) and 17 (Achieve the goals through partnerships).

Note;
CSIRT: Computer Security Incident Response Team.
Organization to implement appropriate responses to information security problems or incidents

JPCERT/CC Initiatives

CSIRT Capacity Building

JPCERT/CC has been providing training targeting National CSIRTs including basic CSIRT operation, international operation, incident response. This also includes network traffic analysis and malware analysis hands-on exercises. In the past years, JPCERT/CC has conducted this type of training in some Asian countries (Vietnam, Indonesia, Laos etc.) and also for African CSIRT communities.



Message from the ASEAN Secretariat

Cybersecurity issues are becoming more pervasive and sophisticated due to the increase in digital connectivity and the growing adoption of emerging technologies such as cloud computing, blockchains and artificial intelligence. As the ASEAN Member States are geared towards establishing a regional digital economy, it is imperative to intensify collective efforts to realise the vision of building a peaceful, secure and resilient regional cyberspace that serves as an enabler of economic progress and betterment of living standards for all. The ASEAN-Japan Cybersecurity Cooperation plays an instrumental role in supporting ASEAN in enhancing its preparedness to respond to cyber threats by implementing capacity-building and confidence-building measures across the region.

〈Policy Reference〉
Preparation of the ASEAN Cyber Security Handbook
Create and update policy references on key Japanese and ASEAN cybersecurity policy items

Senior Officer – Digital Economy
Division The ASEAN Secretariat
Arthur Glenn Maail

Initiatives by ASEAN Countries

Brunei Darussalam

Cybersecurity challenges and future needs

- Rapid changes in cybersecurity and cyber crime threats that evolves constantly and become sophiscated and organised
- Transnational / cross border cybersecurity issues
- Lack of awareness in cybersecurity among the citizen
- Lack of cybersecurity professionals and expertise

Cyber Battle: Capture The Flag 2022 Competition.

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	・Drafting of Cyber Security Order (CSO) for the protection of CII (2020)	・Gazzeting the new CSO & implementation
Technical	・Cybersecurity Incident Reporting procedure for Government (2021)	・Conducting cyber exercises for government
Organizational (Including strategy)	・ISO 27001 ISMS Certification for CSB Core Services (2023) ・ISO 17025 Digital Forensics Lab Acreditation (2022) ・Drafting of National Cybersecurity Strategy for 2023-2027 (commenced drafting in 2020) ・Brunei National Cybersecurity Framework (BNCSF) (2017.10) ・Creation of Cyber Security Association (2022.11)	・Maintaining ISO 27001 & ISO 17025 certification ・Execution of National Action Plan in the National Cybersecurity Strategy ・Reviewing of BNCSF to align with Cyber Security Order ・Association registration & operation
Capacity Development	・Critical Information Infrastructure Workshop for CII owner (2022.10)	—
Cooperation (Between organizations)	・MOU between CSB and Brunei Darussalam Central Bank in cybersecurity (2021.12) ・Letter of Engagement (LOE) between CSB and Telcos (UNN) for joint cybersecurity awareness (2022.11)	・MOU with Universiti Teknologi Brunei in cybersecurity ・MOU with Universiti Brunei Darussalam in cybersecurity

Cambodia

Cybersecurity challenges and future needs

〈Challenges〉

・Lack of proper legislations, strategy, standards and guidelines.
・Limited human resources in cybersecurity.
・Inadequate technology solutions and industry participation.
・Attack sophistication Vs. Knowledge and skill.
・Cooperation among relevant organizations still limited.

〈Needs for cooperation〉

・Developing Cybersecurity strategy, standard and guidelines.
・Developing Cybersecurity workforce program.
・Capacity building and awareness raising.
・Sharing information and best practices.

Cyber Angkor TTX2018

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	・Cybersecurity law (zero-draft) ・Cybercrime law (draft) ・Personal Data Protection law (zero-draft) ・FinTech Policy (draft)	・Revising and adopting the drafted laws
Technical	・Security Operation Center Team ・Cambodia Computer Emergency Response team	・Enhancing and improving the capacity
Organizational (Including strategy)	・Cambodia Digital Economy and Society Policy Framework 2021-2035 (2021.05) ・Cambodia Digital Government Policy 2022-2035 (2022.01)	・Establish Digital Security Committee
Capacity Development	・Digital Skill Essential training program for government officers. ・Cybersecurity awareness for all ・Cybersecurity competition	・Cybersecurity Workforce Development ・Cybersecurity Competency Framework
Cooperation (Between organizations)	・The Economic and Social Development Program (Japanese Government Grant) ・Project for improvement of Cyber Resilience (JICA Project for 3 Years 2023-2026) ・ASEAN-JAPAN, ASEAN-CERT, ASEAN CYBER-CC, ARF, ANSAC	・Improving SOC operation and response capability ・CSIRT development program ・ASEAN-CERT will be established

Indonesia

Cybersecurity challenges and future needs

〈Cybersecurity challenges〉

・Competent human resources on cyber security such as, cyber incident handling, technical risk assessments, cybersecurity strategy and policy development, etc

・Lack of policy framework and national regulation on cybersecurity and cryptography

・Development of new cyber threats in region, such as AI, advanced technology, online-scam, etc

〈Future needs〉

・Bilateral cooperation with other established cybersecurity policies countries

・Sharing information and experiences through fora international, in regional and multilateral

・Assistance from other country to provide advanced exercise and capacity building activities

14th ANSAC 2023, Bali

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	・Presidential Regulation Number 82 Year 2022 on CII Protection	・Internal regulations on CII Protection, CII Identification, CSM Measurement, Cyber Incident Handling, and Human Resource Capacity Building on Cybersecurity and Cryptography
Technical	・National Security Operational Center (2019-present)Nat-CSIRT, Gov-CSIRT, Org-CSIRT	・Establishment of 121 sectoral CSIRT in Indonesia ・Establishment of IKN smart city project
Organizational (Including strategy)	・Presidential Regulation Number 47 Year 2023 on National Cybersecurity Strategy and Crisis Cyber Management	・Plan of Action (PoA) of National Cybersecurity ・Internal regulations on Crisis Cyber Management
Capacity Development	・Actively participate on capacity building development from various programs both bilateral and regional such as AJCCBC, ASCCE, JICA-UI, JICA Scholarships Program, Cybersecurity Capacity Building for ISP Sector, ASEAN Cyber Shield (ACS)	・Request assistance from Japan to develop technical in advance level ・Following all relevant training and capacity building
Cooperation (Between organizations)	・MoU between IDSIRTII/CC – JPCERT ・ASEAN (ANSAC, ASEAN-CERT, ASEAN CYBER-CC, ARF, ADGSOM)	・Renewal MoU between IDSIRTII/CC – JPCERT

Lao P.D.R.

Cybersecurity challenges and future needs

〈Cybersecurity challenges〉

・Development of human resource to be cybersecurity expertise

・Define and develop cybersecurity policy for CII sectors

・Establishment of Cyber Security Operation Center to server/monitor public and private network

・Lack of cyber security tools and Difficulty tracking cyber criminals

・Fake news and Disinformation, Information Sharing from Service provider and social media Platform company and Chatting platform company

〈Future needs for cooperation〉

・Need bilateral cooperation in capacity building

・Need assistance to develop open source software in monitoring cyber-attack

・Need cybersecurity expertise to develop Legislation, Law, strategy, policy

LaoCERT
Lao Computer Emergency Response Team

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	・Law on Prevention and Combating Cyber Crime(2015) ・Law on data Protection(2017)	・Drafting on Cyber security Law
Technical	・Study the possibility of initial establish Cyber Security Operation Center: CSOC ・Attended JICA, METI on capacity building project	・Request assistance from Japan to support on technology, tools, etc..,
Organizational (Including strategy)	・Established LaoCERT in 2012 ・Established Department of Cyber Security under ministry of Technology and Communications in 2022	・Drafting National Cyber Security Strategy
Capacity Development	・Cybersecurity capacity building: Technical skill in incident handling, incident response, computer forensic, network forensic, cyber exercise and etc..,	・Request assistance from Japan to develop technical in advance level
Cooperation (Between organizations)	・MoM with JPCERT/CC ・Information sharing with JPCERT/CC ・Implemented Cybersecurity Activities with NISC, ASEAN-Japan	・Develop Cybersecurity awareness

Initiatives by ASEAN Countries

Malaysia

Cybersecurity challenges and future needs

〈Challenges〉

- Cyber security governance;
- Human resources and technical experts;
- Limited legal frameworks;
- Lack of public awareness;
- Rapidly evolving nature of cyber threats; and
- Limited financial resources.

〈Future needs〉

- More technical trainings and capacity building;
- Provide Train-of-Trainers in niche areas such as Industrial Control System (ICS) and Emerging Technologies;
- Collaboration with universities to develop future cyber workforce;
- Partnership with industries on expert and technical capacity; and
- Collaboration with cyber security players for a conducive cyber ecosystem.

CYDES Opening Speech

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	· National Cyber Security Policy (2010) · Cabinet Decision on the Implementation of ISO/IEC 27001: Information Security Management Systems Standard to Critical National Information Infrastructure (CNII) Agencies (24th February 2010) · Personal Data Protection Act 2010 · National Cyber Crisis Management Plan (NCCMP) (2011) · National Security Council Directive No. 24: Policy and Mechanism of the National Cyber Crisis Management (2011) · National Cryptography Policy (2013) · National Security Council Directive No.26: National Cyber Security Management (2021)	· Malaysia Cyber Security Bill · New guidelines and circulars on cybersecurity
Technical	· Establishment of Malaysia's National Cyber Coordination and Command Centre (NC4) · Public Sector Cyber Security Framework 2016 · Issuance of Technical Advisories for CNII Agencies · Technical Code-Requirement for Information and Network Security · Public Sector Information Security Management on Cloud Computing Guidelines · Public Sector Cyber Security Incident Management Circular 2022 · Establishment of National Computer Emergency Response Team (CERT)	· Enhancement of Malaysia's National Cyber Coordination and Command Centre(NC4)
Organizational (Including strategy)	· Establishment of National Cyber Security Agency (NACSA) - 2017 · National Cyber Security Policy 2010 · Malaysia Cyber Security Strategy 2020-2024 · Development of National Cyber Security Awareness Masterplan	· Streamlining the Malaysia's governance structure in cybersecurity · Dedicated Operational Expenditure for cyber security
Capacity Development	· National Cyber Drill Exercise (X-Maya) · Sectoral Cyber Drill Exercise · CYDES 2020 · ICTSO 2022 · Industrial Talk on Network Security · Certification Training on ISMS and BCMS (Every Year)	· CYDES 2023 · ICTSO 2023
Cooperation (Between organizations)	· ASEAN Cybersecurity Cooperation Strategy 2021-2025 · ASEAN Regional Action Plan (RAP) Matrix on the Implementation of the UNGGE Norms of Responsible State Behaviour in Cyberspace · Malaysia-Japan Cybersecurity Policy Dialogue	—

Myanmar

Cybersecurity challenges and future needs

- Insufficient human resources
- Limited in terms of regulatory and policy implementation due to statutory requirements.
- Lack of formalized cybersecurity law leads to regulatory limitations to regulate the cybersecurity industry and cyber related issues.
- Requirement for organizational structure of dedicated authority for cyber security bodies such as CSIRT, ISAC and Security Audit.
- Capacity Development Training Programs from JICA as usual before covid-19 pandemic.
- Capacity Building Support for both policy level and operational level.
- Further technical cooperation.

Myanmar Cybersecurity Challenge(2023)

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	· Computer Science Development Law (1996) · Electronic Transaction Law (2004), Amendment in (2014, 2021) · Telecommunications Law (2013) Amendment in 2017 · Cyber Security Policy is approved by the meeting of the Government of the Union of Myanmar No. (9/2022) held in December, 2022.	· Cyber Security Law
Technical	· Myanmar Computer Emergency Response Team (mmCERT/cc) · Government Security Operation Center (GSOC)	· To encourage for establishing sectoral CSIRTs among government agencies. · 24/7 protection for government agencies as per demands.
Organizational (Including strategy)	· Ministry of Transport and Communications - MoTC is responsible for policies related to ICT including information security in Myanmar. · Information Technology and Cyber Security Department - ITCSD is responsible for the cooperation and coordination of E-Government Projects/ Process of different departments, implementation of E-Government Projects, ICT Standardization, Supervision and Technical advisory of Cyber Security and implementing the Cyber Security Law, Cyber Policy and Framework. · National Cyber Security Center-NCSC is responsible for creating the environment where all ministries can provide online services securely and all citizens can access E-Government services safely as well as for rolling out cybersecurity awareness program through the country.	· To expand the organization structure according to the Cyber Security Policy.
Capacity Development	· Jointly developed with Japan and Myanmar, "Let's Learn Cyber Security" Awareness Booklet was published. Reprinted again in 2022 and distributed in " Youth, Literature and Art Show" at MICC-2, Nay Pyi Taw. · Contributes in Joint Awareness Raising Activity for "Cyber Security for Mobile Devices" E-booklet in 2021. Myanmar participated with the topic : "Ransomware in Mobile Devices". Reprinted in A5 Size Booklets and disseminated to government organizations in 2022. · Myanmar Cybersecurity Awareness Video Competition-2023 is being held in order to choose the winner to be able to participate in ASEAN-JAPAN Cybersecurity Awareness Video Competition. · JPCERT/cc and mmCERT/cc jointly organized Network Forensics, Malware Analysis, Advanced Malware Analysis, Incident Handling and Advance Incident Handling Courses in 2011, 2012, 2013 and 2015. There were above 250 attendees from government agencies and private financial sectors throughout these years. · Employees from ITCSD have been being sent to attend AJCCBC Cyber Security Technical Training Courses both on-site and online since 2019. · Sent attendees for "Defense Practice against Cyber Attacks" Training Courses in 2019, 2020 and 2021 both on-site in Japan and virtually. · With the support of AJCCBC, NCSC provided "Self-learning Training Course Localized Version" to employees from government agencies in 2020 and 2021. · By applying the knowledge learnt from AJCCBC courses, NCSC provides "Incident Handling-Intrusion Detection Courses" at universities in 2019, at Ministry of Information in 2020 and at Training Center of ITCSD in 2022 for the employees from government organizations. · Myanmar Cyber Security Challenges are held annually except during the covid-19 circumstances. The 7th MCSC was held on 5th August 2023 for selecting participants for ASEAN Cyber SEA Games and other regional cyber competitions.	· Awareness Booklet and Posters will be produced and disseminated in local exhibitions, workshops and awareness raising programs. · To participate in ASEAN-Japan Cybersecurity Awareness Video Competition-2023. · Cyber Security Awareness Short Movies will be broadcasted and posted this year. · Local trainings, knowledge sharing sessions and awareness raising program will be conducted by applying the knowledge gained through international programs. · To promote the awareness raising programs and events at Universities and High Schools. · To provide Internship program for university students as per request. · To host the Myanmar Cyber Security Challenges every year for enhancing the cyber security skill and building the capacity for cyber security professionals.
Cooperation (Between organizations)	· Joins Meetings, Seminars and Drills as an operational member of APCERT. · Participates in ASEAN Network Security Council (ANSAC) · Contributes in ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC). · Participates in ASEAN-JAPAN Cyber Security Policy Meetings and Working Group Meetings. · Conducts ASEAN-JAPAN Remote Cyber Exercises, ACID Drills, ITU Drill and ASEAN Cyber SEA Game every year. · Jointly organized with MIC of JAPAN and MOTC of Myanmar, "Workshop on Cyber Security in Myanmar" was held in 2019. · Hosted the 4th Senior Level Workshop on International Cybersecurity Policy and Diplomacy for CLMV Countries in 2019. · Co-chaired at the 3rd ASEAN-Japan WG Meeting in 2017, and the 3rd Meeting of ASEAN Cyber-CC in 2022. · Virtually Hosted the 13th ANSAC meeting in 2022.	· To continue the contributions in international, regional and local cooperation in order to strengthen the relationships among the cyber security related organizations.

Philippines

Cybersecurity challenges and future needs

- **Lack of cybersecurity professionals in the country.** In 2016, it has been reported that there were only 84 CISSP certified professionals in the Philippines compared to 107 in Indonesia, 189 in Thailand, and 275 in Malaysia. And not all 84 are based in the Philippines. Most of them were working abroad. At present, the (ISC)2 website shows that there are already 216 CISSPs in the country but the number is still too low to essentially fill up the required number of professionals by the industry. **Partnership could be in the development of education programs for cybersecurity.**
- **Capacity Building for CERTs.** Although Sectoral CERT leads have been identified for each CII, the major challenges are the lack of personnel that could man the CERTs and the absence of security operations centers.
- **The need for cybersecurity standards.** One area where the Philippines scored low in the latest Global Cybersecurity Index (GCI) is the adoption of a national framework for cybersecurity standards. Since last year, DICT has been working on the adoption of cybersecurity standards that would mitigate or prevent cyber-attacks by reducing the risks of ICT equipment and critical assets.

National Cybersecurity Plan 2028
Multi-stakeholders' Consultation
(Visayas Leg)

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	・Enactment of the Cybercrime Prevention Act of 2012 and the Data Privacy Act of 2012 ・Enactment of the DICT Act of 2015 which created the Department of Information and Communications Technology	・Cybersecurity Law ・CII Protection Act (Senate Bill) ・Executive Order Mandating Minimum Information Security Standards for CIIs
Technical	・Creation of the National Computer emergency Response Team (CERT-PH) in 2018 ・Launching of the National Cybersecurity Operations Center (NSOC) in 2018 ・Annual Cyber Drill ・Vulnerability Assessment and Penetration Testing for government agencies ・Recognition of Cybersecurity Assessment Providers	—
Organizational (Including strategy)	・Development of the National Cybersecurity Plan 2022 ・Inclusion of cybersecurity in the 12 Point National Security Strategy ・Inclusion of Cybersecurity in the Philippine Development Plan (PDP) 2028	・Development of the National Cybersecurity Plan 2028 (Expected to be published on May 30, 2023)
Capacity Development	・JICA Technical Capacity Building Project ・Cyber Range Platform ・Cybersecurity Advocacy and Awareness Campaigns	—
Cooperation (Between organizations)	・Creation of the National Cybersecurity Inter-agency Committee (NCIAC) ・Cyber Threat Monitoring and Information Sharing ・National Cybersecurity Inter-Agency Committee (NCIAC)	—

Singapore

Cybersecurity challenges and future needs

〈Cybersecurity Challenges〉

Cyber threats targeting Operational Technology (OT) systems have evolved in capability and impact

・OT systems usually underpin the provision of essential services, any successful compromise can have potentially serious consequences

Threat of ransomware has expanded to include nearly all industries and sectors

・Of concern is the trend of ransomware groups pivoting to target large essential service providers

Geopolitical tensions and the role of non-state actors in a conflict

・Many non-state actors have significant heft and influence that could shape the direction and scale of a conflict

〈Future Risks〉

・**Ransomware for Reputation (R4R) -** Ransomware groups increasingly turning their attention to data exfiltration instead of encryption, extorting companies to pay up to avoid reputational damage

・**Artificial Intelligence (AI) as a double-edged sword -** AI could amplify the capabilities of cyber threat actors

・**Quantum Computing and Digital Security -** Threat actors could potentially exploit quantum computing to compromise encryption algorithm that safeguards websites and mobile applications

7th ASEAN Ministerial Confernce on Cybersecurity

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	・Cybersecurity Act (2018) ・Cybersecurity Code of Practice for Critical Information Infrastructure(CII)2.0 (2022) ・Personal Data Protection Act (2012) ・Computer Misuse Act (1992)	Ongoing review of Cybersecurity Act 2018
Technical	・Singapore Computer Emergency Response Team (CERT) ・ASEAN CERT Incident Drill (ACID) ・ASEAN Information Sharing Sessions by SingCERT ・Security-by-Design Framework for CIIs ・Guide to Conducting Cybersecurity Risk Assessment for CII ・Guidelines for CII Owners to Enhance 5G Use Cases ・Cybersecurity Audit Guidelines for CII ・Guide to Cyber Threat Modeling for CII ・CII Supply Chain Programme Paper ・Operational Technology Cybersecurity Competency Framework ・Cybersecurity Labelling Scheme for IoT and Medical devices ・Singapore Common Criteria Scheme ・Licensing Framework for Cybersecurity Service Providers ・Monthly CyberSense Newsletter on latest cybersecurity topics, trends, and technologies ・Cybersecurity Certification Scheme Cyber Essentials Mark Cyber Trust Mark ・Cybersecurity Toolkits for Organisations ・Cybersecurity Health Plan for Organisations	—
Organizational (Including strategy)	・Singapore Cybersecurity Strategy (2021-2025) ・Singapore Operational Technology Cybersecurity Masterplan ・Singapore Safer Cyberspace Masterplan ・Annual Singapore Cyber Landscape (2016-2022)	—
Capacity Development	・ASEAN-Singapore Cybersecurity of Excellence Capacity-building programmes for ASEAN Member States and other international partners, including the UN-Singapore Cyber Fellowship ・CSA Academy ・National and Sectoral level Cyber Exercises ・Public Awareness Raising (GoSafeOnline website) ・SG Cyber Talent Development Fund ・SG Cyber Series (Talent, Youth, Olympians, Educators, Women, Leaders)	—
Cooperation (Between organizations)	・Singapore International Cyber Week ・OT Cybersecurity Expert Panel ・Cybersecurity Industry Call For Innovation ・Innovation Cybersecurity Ecosystem at Block 71 ・National Cybersecurity Research & Development Programme ・National Integrated Centre for Evaluation by CSA and Nanyang Technological University ・CSA works with the sector leads of the 11 identified critical sectors to protect, respond and investigate any cyber-incidents affecting CIIs.	—

Initiatives by ASEAN Countries

Thailand

Cybersecurity challenges and future needs

〈Challenges〉

- Build up all the ecosystem and cyber capacity for all components: people, policy, knowledge, system
- Build up synergy via strong partnership and integrated effort
- Improved resiliency for CII and government services
- Strive to be world class cybersecurity organizations: improve related agencies and organizations in terms of standards and quality of services offers

〈Needs for cooperation 〉

- Building trust and Information sharing between country
- International Table Top Exercise
- International collaboration to address cyber threat
- Training and workshop for International Law of Cyber Operations
- Cooperating with industries for training cybersecurity in part of OT system

AJCCBC Opening Ceremony 2018

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	· Computer Crime Act 2007, 2017 · Personal Data Protection Act 2019 · Cybersecurity Act 2019 (National Cyber Security Agency : NCSA)	· Implementing and enforcing secondary legislation, regulations, and guidelines to increase cyber security standards and maturity. · Providing minimum security standard for critical information infrastructure organization
Technical	· Thailand Computer Emergency Response Team (ThaiCERT) · Establish Sectoral CERT	· Enhancing cybersecurity capabilities of ThaiCERT in order to be prepared for future threats. · Promoting and supporting threat information sharing
Organizational (Including strategy)	· Critical Information Infrastructure (CII) organizations stipulated by the act must comply with the standard framework of security requirements · NCSA will formulate a code of practice and standard framework of cybersecurity as a guideline for organisations of CII. · Announcement of the National Cybersecurity Committee on Cyber Security Policy and Action Plan (2022 - 2027) "Cybersecurity for Thailand's critical services to ensure economic and social sustainability" · Advancing the Cybersecurity Policy and Action Plan for long-term success and progress. · Promoting cyber resilience for government services and critical information infrastructure	· Providing minimum security standard for critical information infrastructure organization · Establishing a regulatory structure and legal framework for critical information infrastructure organization · Protecting government agency's data systems and networks
Capacity Development	· Building country's cybersecurity capacity by integrating workforce, knowledge, and technology, to develop cybersecurity innovation · Developing the competence of the cybersecurity workforce through different programmes · NCSA developed cybersecurity skills for organisations of CII to meet international standards through intensive capacity-building programmes targeting 2,250 attendees, including 400 specialists and executives in 2022 · NCSA and JICA signed the Record of Discussions for the Project for Enhancing ASEAN-Japan Capacity Building Programme for Cybersecurity and Trusted Digital Services operated by AJCCBC	· Increasing cybersecurity workforce · Raising cybersecurity awareness and skill · Promoting cybersecurity research and development, including innovation
Cooperation (Between organizations)	· Seeking cooperation and partnership from both domestic and international organizations. · Integrating domestic and international collaboration in preparation for cyber threat response and recovery of critical services to normal operations · NCSA is responsible for providing assistance to prevent and mitigate risks from cyberthreats to 7 sectors of CII: national security, public service, banking and finance, information technology and telecoms, transportation and logistics, energy and public utilities, as well as public health.	· Promoting and supporting public - private partnership · Coordinating international collaboration to address cyber threat

Viet Nam

Cybersecurity challenges and future needs

- Rapid changes in cybersecurity and cyber crime threats that evolve constantly and become sophisticated and organized

- Developing standards and guidelines.
- Developing cybersecurity workforce program.
- Capacity building and awareness raising.
- Sharing information and best practices.

The Office of Ministry of Communication and Information

Efforts and future plans

Category	Details of Implementation	Future Plan
Legal	· Law on Cyber Information security 2015. · Law on Cybersecurity 2018	· Proposing new cyber security policies, regulations tackle with emerging cybersecurity challenges.
Technical	· Viet Nam Cybersecurity Emergency Response Team/Coordination Center - VNCERT/CC · National Cyber Security Center - NCSC	· Improving SOC operation and response capability · CSIRT development program
Organizational (Including strategy)	· Authority of Information Security (AIS) is government authority in charge of state administration in cyber security field of Viet Nam.	· Implementing the Viet Nam cyber security strategy Promoting the implementation of National Digital Transformation.
Capacity Development	· Proposing new cybersecurity policies, regulations and measures on emerging subjects. · National Master plan by 2025 on developing cyber security human recourse; cyber security awareness raising; and Cyber Resilience	· Implementing the Master plans and review the result year by year
Cooperation (Between organizations)	· ASEAN (ANSAC, ASEAN-CERT, ASEAN CYBER-CC, ARF); · ASEAN + (ASEAN-Japan,Us...);ITU; .. · ASEAN; FIRST; CAMP.	· Improving SOC operation and response capability · CSIRT development program

Examples of Major Initiatives by Japan

Initiatives by the Ministry of Internal Affairs and Communications

Cooperation for building cybersecurity capacity in ASEAN

The ASEAN-Japan Cybersecurity Capacity Building Centre was established in Bangkok, Thailand, and the opening ceremony of the Center was held on September 14, 2018.
The Ministry of Internal Affairs and Communications (MIC) will take this opportunity to further strengthen its cooperation in building cybersecurity capacity in ASEAN.

(1) Past activities and results

Cybersecurity-related projects implemented in the ASEAN region from 2009 to date
<AJCCBC>
Year of Activity ▶ 2018-2022
Activities ▶ Ensuring the smooth operation of the AJCCBC
Results ▶ Over 1,000 students have participated in the AJCCBC.
Candidates for Distinguished Service (Award Recipients) ▶
<AJCCBC>ETDA Executive Director Dr. Chaichana Mitrpant and other officials

(2) Projects in planning or under consideration

Future plans and expectations (e.g., Awareness issues regarding ASEAN)
<Expansion of AJCCBC activities>
Increase participation in existing activities ▶
Promote participation of CII ICT staff and government officials
Future expansion of the AJCCBC's scope of activities ▶
Promote expansion of participants and content of the training exercises.

Note:
JASPER: ASEAN-Japan Technical Cooperation Project to enhance technical cooperation in the field of network security, as agreed in the Joint Statement of the ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation held in September 2013.
Indonesia, Singapore, Thailand, Philippines, Malaysia, Myanmar and Lao P.D.R. participated (Myanmar and Lao P.D.R. have participated for DAEDALUS only)

Launch of a new project at the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)
On June 19, 2023, a ceremony was held at the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) to launch the Japan International Cooperation Agency (JICA) technical cooperation project "Project for Enhancing ASEAN-Japan Capacity Building Program for Cybersecurity and Trusted Digital Services". Through providing exercises to the AJCCBC and enhancing the exercise program, we will continue to cooperate in building cybersecurity capacity in ASEAN.

METI Initiatives

JP-US-EU ICS Cybersecurity Week for the Indo-Pacific Region

METI and ICSCoE, in collaboration with the government of the United States (DHS/CISA, DOS) and the European Commission (DG CONNECT), will host the 6th JP-US-EU Industrial Control Systems (ICS) Cybersecurity Week in October 2023.

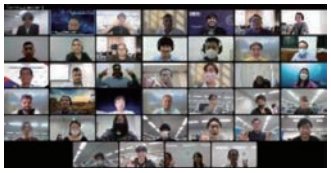
〈Date〉 Oct 9-13, 2023
〈Outline〉 The event was held in Japan, with approximately 40 core participants from the Indo-Pacific region, including ASEAN member states, India, Bangladesh, Sri Lanka, Mongolia, and Taiwan, who participated in practical exercises. In addition,cybersecurity-related seminars, including discussions on current trends such as ransomware and cyber incidents, were conducted by experts from Japan, the U.S., and the E.U.

Last year's exercise

Masahiro Uemura
Deputy-Director General, METI

Eric Goldstein
Executive Assistant Director for Cybersecurity, CISA

Lorena Boix Alonso
Director, DG CONNECT



Participants from the Indo-Pacific Region

Ministry of Defense Initiatives

Cyber Security Capacity Building Support Project

Cyber Security Related Projects Conducted in the ASEAN Region

Year of activity	FY 2017 - FY 2022 (project ended in FY 2022)
Activities	To help improve the cybersecurity capabilities of the Viet Nam People's Army, three seminars were held to provide basic knowledge and skills. This was followed by a retention review with observers from the Australian Defense Force.
Achieved	After confirming the level of retention, we confirmed that the results of the three seminars were well received. As a result, the cybersecurity capabilities of the Viet Nam People's Army have improved.

Year of activity	FY 2021
Activities	In February 2022, a seminar (Sharing of knowledge and practical skills necessary to deal with incidents) to improveincident response capabilities was conducted online for ASEAN countries.
Achieved	20 participants understood the basics of cyber security
Future Plans	The second program will be held in FY2023.

Looking ahead to the next decade

Chief Digital Officer
Japan International
Cooperation Agency (JICA)
Hitoshi Tojima

Based on its experiences in cybersecurity cooperation with partner countries, JICA developed the “Cluster Strategy for Cybersecurity ” in December 2022. The strategy refers to the ITU's Global Cybersecurity Agenda model and presents four development stages in the five capability elements, allowing assessment of the situation of a target country and optimizing cooperation.
Cooperation with ASEAN countries is also expanding, with collaboration with the ASEAN-Japan Cybersecurity Capacity Building Center (AJCCBC) set to begin in 2023, aiming to train more than 500 personnel over the next four years.
JICA will continue to cooperate with the Government of Japan and its partners for further development of ASEAN countries, with the aim of realizing a society capable of responding to increasingly serious threats in cyberspace and protecting people's lives and dignity (“Cybersecurity for All”).
Cluster Strategy for Cybersecurity Cyberse

Director,
Global Coordination Division.
JPCERT/CC
Koichiro Komiyama

Looking back, it has been a challenging decade. UN Secretary-General Guterres expressed that the world is afflicted with a "Trust Deficit Disorder" that also applies to the cyber domain. Over the past decade, countless state-sponsored cyber attacks and mass surveillance activities have come to light. Cross-border cooperation and trust has been questioned.
Looking up front, the future of the ASEAN-Japan relationship is bright. ASEAN and Japan have nurtured friendship despite the international community suffering from a trust deficit. I have true friends in every ASEAN member states, with whom I can consult without reservation, regardless of the affiliation or the political shifts in play. I look forward to forging new cooperation between ASEAN and Japan alongside long-standing friends who have participated in this conference and the new friends we have yet to meet.

Professor,Graduate School of
Information Science and
Technology,
The University of Tokyo
Hiroshi Esaki

The Internet has interconnected digital resources built and operated by diverse organizations, and continuously created a sharing economy-type digital infrastructure across the globe. As a result, all people and all digital devices (called as Things) on the earth have been connected to the Internet across the national borders, and have delivered to enable free data exchange. We now have to implement appropriate level of cybersecurity that assumes that everyone and every single digital device, which have not been expected to be connected, will be connected to the Internet. More than ever before, we must collaborate and cooperate together, encourage new colleagues participation to work together so as to create a better and brighter global digital space, fulfill our responsibility, and hand it over to the next generation.