Enhancing the Government-Industry-Academia Collaboration from Thailand to ASEAN

November 8th, 2022

DEGUCHI Satoshi (Sato)
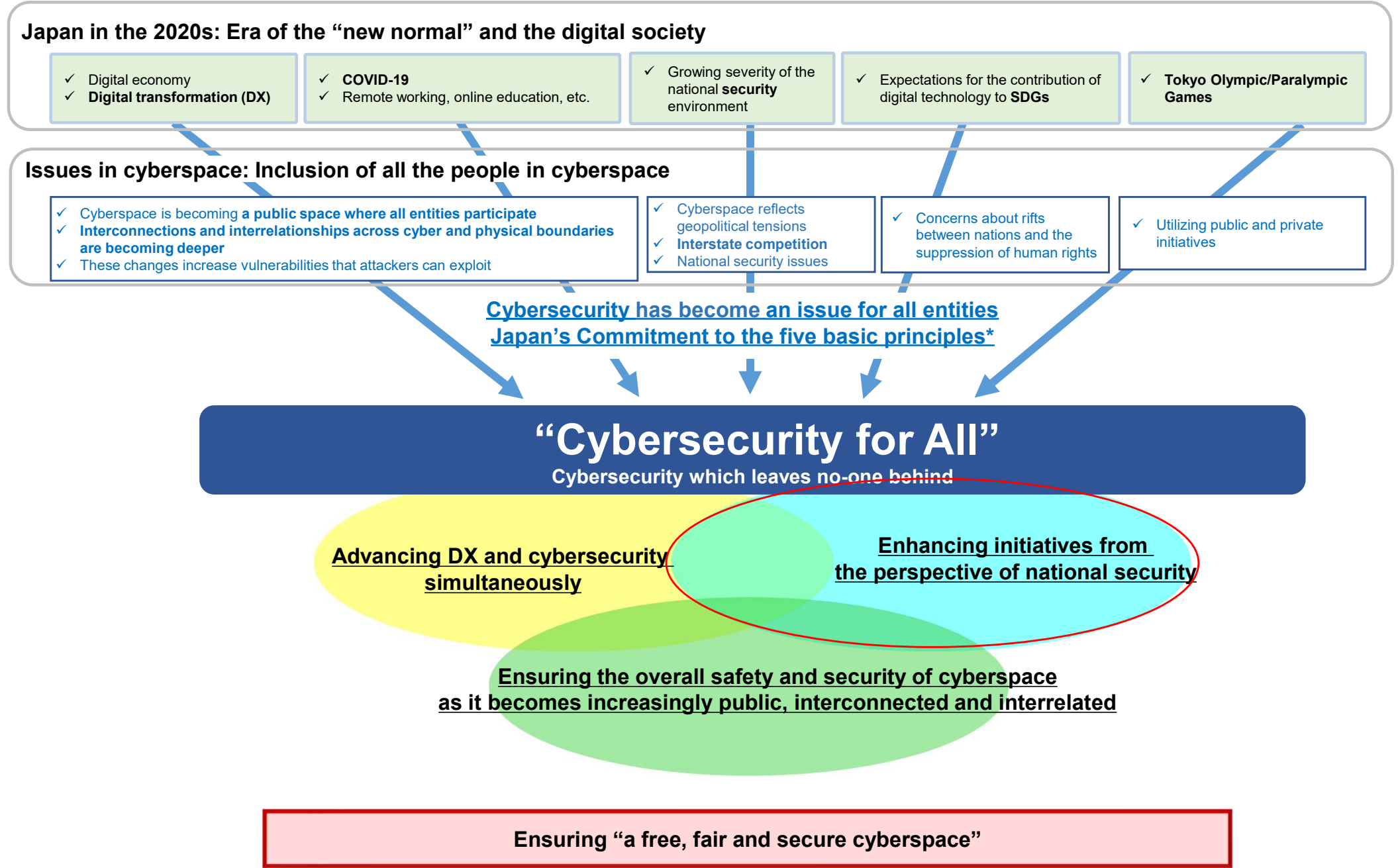
Deputy Counsellor for International Strategy

NISC, Japan

Have you ever seen this logo ?

Do you know what is AJCCBC ?

Issues and Direction of Japan's Cybersecurity Strategy 2021 **NISC**

Japan in the 2020s: Era of the "new normal" and the digital society

- ✓ Digital economy
- ✓ **Digital transformation (DX)**

- ✓ **COVID-19**
- ✓ Remote working, online education, etc.

- ✓ Growing severity of the national **security** environment

- ✓ Expectations for the contribution of digital technology to **SDGs**

- ✓ **Tokyo Olympic/Paralympic Games**

Issues in cyberspace: Inclusion of all the people in cyberspace

- ✓ Cyberspace is becoming **a public space where all entities participate**
- ✓ **Interconnections and interrelationships across cyber and physical boundaries are becoming deeper**
- ✓ These changes increase vulnerabilities that attackers can exploit

- ✓ Cyberspace reflects geopolitical tensions
- ✓ **Interstate competition**
- ✓ National security issues

- ✓ Concerns about rifts between nations and the suppression of human rights

- ✓ Utilizing public and private initiatives

Cybersecurity has become an issue for all entities
Japan's Commitment to the five basic principles*

"Cybersecurity for All"
Cybersecurity which leaves no-one behind

Advancing DX and cybersecurity simultaneously

Enhancing initiatives from the perspective of national security

Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

Ensuring "a free, fair and secure cyberspace"

* Assuring the free flow of information, the rule of law, openness, autonomy, and collaboration among multi-stakeholders

Basic Policy on Cybersecurity Capacity Building Support for Developing Countries

NISC

(Dec. 14, 2021 Approved by the Cybersecurity Strategic Headquarters)

- In December 2021, the government of Japan decided on the Basic Policy on Cybersecurity Capacity Building Support for Developing Countries.
- While the Japanese government has continued to provide the support to the governments of ASEAN countries, Japan will strengthen the support to the private sector, including critical infrastructure providers, through government-industry-academia collaboration.

Importance of support	Approaches
1. Reducing international cybersecurity vulnerabilities and risks. 2. Ensuring the stability of the lives of residents and the activities of companies in recipient countries. 3. Obtaining general understanding of the basic principles of assurance of the free flow of information and the rule of law. 4. Developing a foundation for Japan's industry to operate locally. 5. Contributing to the reinforcement of government policies. (Free and Open Indo-Pacific, etc.)	**1. Support for ensuring cyber hygiene through the protection of critical infrastructure and other means** • enhancing support for critical infrastructure, an area where there are growing needs for supporting measures in each country based on the relationship. • expanding the scope of support in the Indo-Pacific region based on past achievements and experiences in capacity building support in the ASEAN region. **2. Support for measures against cybercrimes** • providing training related to criminal justice in collaboration with the United Nations and others. **3. Sharing understanding and cyber situational awareness of international rules and confidence building measures** • enhancing capacity building support on application of international law and the norms. • securing 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** • collaborating even more closely between relevant ministries for growing needs for support in the critical infrastructure and other fields. • developing human resources to support the activities of Japanese businesses overseas over the medium to long term.

ASEAN-Japan Cybersecurity Policy Meeting

- ASEAN-Japan Cybersecurity Policy Meeting (AJ-CPM) is a framework of Cybersecurity Authorities of ASEAN Member States and Japan for promoting cybersecurity policy cooperation.
  - NISC, Japan serves as secretariat of AJ-CPM.

- The AJ-CPM has been established in 2009 and acknowledged at "ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation" in 2013.
  - The "Joint Ministerial Statement" of the Meeting encouraged joint effort in the following areas.
    - Creating a secure business environment
    - Building a secure information and communication network
    - Enhancing capacity for cyber security

"We believe that a secure cyberspace is one of the major drivers in innovation as well as being essential in promoting social and economic activities and strengthening ASEAN connectivity"

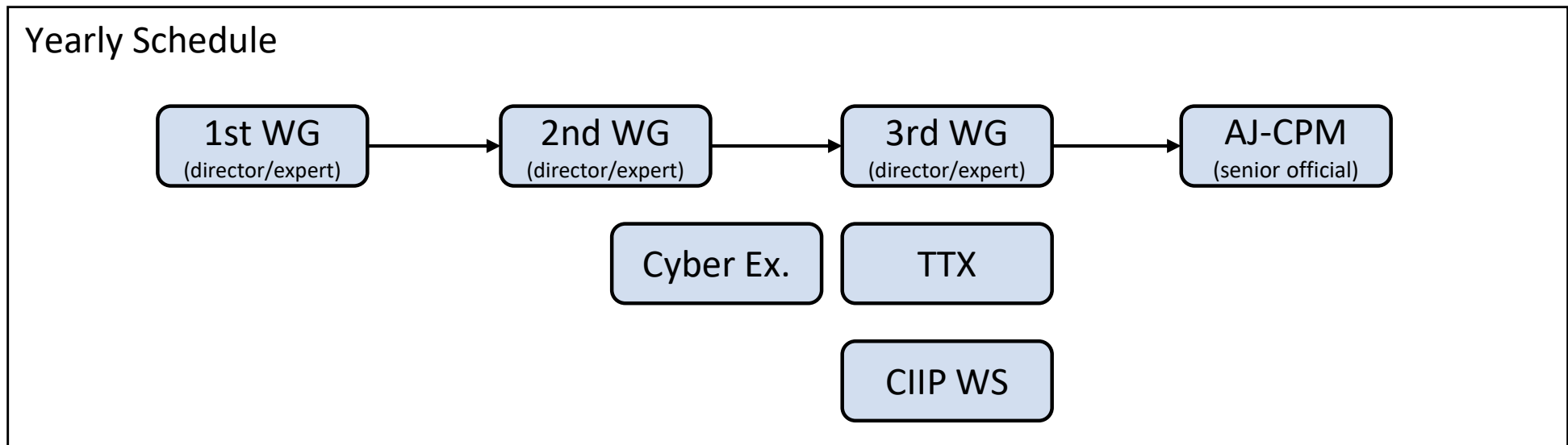# Working Group Meetings and Events

- The AJ-CPM has established its Working Group in 2014 to plan and implement projects.
  - The WG have 3 meetings a year.

- The AJ-CPM conduct 3 events yearly.
  - Cyber Exercise
  - Face-to-Face Table Top Exercise (TTX)
  - CIIP Workshop

WG Meeting

Table Top Exercise

Yearly Schedule

| 1st WG (director/expert) | → | 2nd WG (director/expert) | → | 3rd WG (director/expert) | → | AJ-CPM (senior official) |

| Cyber Ex. | TTX |

| CIIP WS |

Collaborative Activities (CAs) under AJ-CPM

- The AJ-CPM has endorsed to promote 10 CAs in 2023.
    - CA is a yearly activities that all Member Agencies are participating.
    - Each CA is lead by its Lead Country, and its output should be reported to AJ-CPM.

    1. Remote Cyber Exercise
    2. TTX
    3. CIIP Workshop
    4. Joint Awareness raising
    5. Capacity Building
    6. Voluntary Mutual Notification Program
    7. AJ Cybersecurity Reference
    8. WG Steering
    9. **Joint-Government-Industry-Academia (Since 2021)**
    10. **50th Year Commemorative Activity (Since 2023)**

Member Agencies of AJ-CPM

- The AJ-CPM is a closed meeting consist of senior officials of each country's Cybersecurity Agency and ASEAN Secretariat.
  - The member agencies can invite officials of their cooperative agencies.

Country	Member Agencies of AJ-CPM		Cooperative Agency
	Cybersecurity Authority	National CSIRT	
Brunei	NSC	BruCERT	
Cambodia	MPTC	CamCERT	
Indonesia	BSSN	ID-SIRTII/CC	MCIT
Japan	NISC	NISC, JPCERT/CC	MIC, METI, MOFA, JPCERT/CC, JICA, IPA, JC3
Laos	MPT	LaoCERT	
Malaysia	NACSA	NC4	MCMC
Myanmar	MOTC, NCSC (of MOTC)	mmCERT	
Philippines	DICT	NCERT	
Singapore	CSA	SingCERT	MCI
Thailand	NCSA	ThaiCERT	ETDA
Vietnam	AIS	VNCERT	

* Cooperative Agencies are not limited to that shown on the table.

Cybersecurity Capacity Building from Thailand (AJCCBC)

- AJCCBC implements human resource development programs on cybersecurity in ASEAN with the support of the Japanese government.
- ETDA of Thailand established the centre based on the agreement of the 17th ASEAN and Japan Telecommunications and Information Technology Ministers Meeting in December 2017. From October 2022, the centre has been operated by NCSA.

Main activities

1. Cybersecurity Hands-on Exercises

Hands-on exercise for government organizations and critical infrastructure providers
- Cyber Defense Exercise with Recurrence (CYDER)
- Digital forensics
- Malware analysis

2. ASEAN Youth Cybersecurity Technical Challenge (Cyber SEA Game)

Competition of cyberattack handling that promotes the ability of young engineers and students selected from ASEAN member states (Once a year)

3. Cybersecurity Online Training Programs

Since COVID-19 pandemic, online training courses have been provided.

Ministers Meeting (Dec 2017)

CYDER

9

AJCCBC is the Capacity Building Centre for ASEAN.

AJCCBC Operator

Capacity Building Coordination

AJCCBC program development assistance

Cybersecurity Development Assistance

Thank you !