Interactive Workshop on Strengthening the Security and Resilience of ICT-Enabled CI

Singapore and the European Union

Workshop Report

1. Background

In 2019, in the context of ASEAN Regional Forum (ARF) work on Confidence Building Measures (CBMs), Singapore and the European Union identified the topic of ICT-enabled critical infrastructure as a key area of cooperation. The initiative aims to reduce misunderstanding, misperception, and miscalculation, as well as the risk of conflict stemming from the use of ICTs through capacity and awareness building where critical infrastructure security and resilience is concerned, and through closer cooperation and understanding between States in the event of a malicious ICT-enabled activity.

Building on a first workshop on the protection of ICT-Enabled Critical Infrastructure held in 2021, **Singapore's Cyber Security Agency (CSA) and the European Union's External Action Service (EEAS) organised a second iteration** in Singapore **on 6-7 June 2024.**

The second workshop drew from on-going discussions at the United Nations on ICTs and international security and related efforts in the ASEAN region to advance implementation of agreed voluntary and non-binding norms on the responsible behaviour of States in their use of ICTs as well as confidence and capacity building measures relevant to critical infrastructure protection (concept note and agenda in annex 1). In doing so, it sought to exchange national and regional policies, strategies, tools and mechanisms and identify good practices and lessons that can be leveraged to build confidence within and between ARF participating States, and capacity building activities across regions.

2. Key takeaways

Key takeaways from the workshop include the following:

- While certain cybersecurity threats such as **ransomware, malware, phishing, supply-chain attacks and cyber-enabled espionage operations** are on the rise and often require coordinated action at national, regional and international levels, each CI sector — be it energy, healthcare, telecommunications, transportation, financial services,— faces unique threats and vulnerabilities. **Tailored risk management strategies** are necessary to address sector-specific challenges and ensure robust protection.

- Effective resilience of ICT-enabled critical infrastructure requires a **comprehensive approach** that identifies the **opportunities** and **challenges** relevant to **people**, **process** and **technology** within any given CI sector**.** Such a comprehensive approach should also integrate the full cycle of **prevention, detection, response, recovery** into relevant strategies, ensure more systems-based approaches to risk management, including by addressing **dependencies** and **interdependencies** of ICT-enabled CI in and across sectors and countries. In particular, organizations should continuously **adapt** their risk management practices based on insights gained from **past incidents.** This can strengthen resilience and **inform adaptation** or **future development** of national strategies and regulatory frameworks. Integrating after-action reviews into the risk management cycle is key in this regard.

- Specific priorities, such as ensuring greater cybersecurity in OT systems, should figure in national policy so as to ensure dedicated budgetary and other resource allocations.

- **Public-private partnerships** are crucial to strengthening the security and resilience of ICT-enabled CI. They enable sharing of resources, threat intelligence, and facilitate more coordinated and timely responses to incidents. Enhancing **collaboration** between the **public and private sectors** is viewed as critical yet it is difficult to implement in practice. Additional support and training in that context would be beneficial. Regular consultations between the relevant authorities and CI sector operators; certification programmes and economic incentives; secure and shared channels for communicating and sharing threat data, and investment in education and training opportunities are examples of how governments can incentivise more regular and effective communication and collaboration between the two sectors.

- Given the oft-interconnected nature of ICT-enabled critical infrastructure, with some infrastructures providing services across several countries, **regional cooperation** is vital. **Enhanced exchanges** among ARF participating States **on** the evolving threat landscape, **national policies** and **strategies**, **best practices in incident response and recovery** and lessons learnt from past **incidents** bolster cyber security and resilience across all States and contribute to greater trust between counterparts.

- In addition to regional discussions, **exchanges** between **technical, operational and political levels** of cooperation should be sought at national level, as well as between different communities of practice (e.g., technical/ cybersecurity experts, law enforcement, defense, diplomacy). Such exchanges can enable learning from respective progress and challenges, and help **breach silos**, where necessary.

- Continuous training and capacity building for cybersecurity professionals are essential as is **raising the profile** of **cybersecurity as a profession** to aspire to. Investing in **education** at all levels and in **certification programs over the course of careers** would contribute to developing a **skilled workforce** capable to adapt as technology continues to evolve. The conduct of **regular crisis management exercises** would also enable professionals to better manage and mitigate cyber risks.

- **Leveraging advanced technologies** such as artificial intelligence (AI) and machine learning (ML) can enhance risk mitigation capabilities since these technologies can support **early threat detection** as well as timely **response** and **risk mitigation**. Nonetheless, understanding the **risks** and potential **harms** associated with their use should be done in parallel.
- Significant investment in capacity building across all these areas is needed.

3. Possible way forward

The second Workshop benefited from the in-person participation of government representatives from ARF participating States. The workshop demonstrated the importance of continuous knowledge development and exchanges amongst policy and operational experts and between the public and private sectors. Drawing from the key takeaways (above), the workshops discussions (below) and the workshop survey feedback, CSA and EEAS see potential in continuing their collaboration on advancing CBM implementation relevant to critical infrastructure.

In this regard, potential future engagement could include:

- Deep dives on risk and crisis management relative to a specific ICT-enabled CI sector (e.g., a sector that several states depend on such as financial services, telecommunications, including relevant subsea infrastructure, energy, maritime).
- National and regional approaches to crisis management of ICT enabled CI, with exchanges on concrete lessons from past incidents.
- Public-private cooperation for secure and resilient ICT-enabled infrastructure.

As for formats for future collaboration, the June 2024 workshop confirmed the value of in-person engagement and ensuring interactive discussions between speakers and participants from different cyber communities, throughout. Future collaboration could maintain a similar format, eventually bringing the findings of the workshops together in a regional conference on security and resilience of ICT-enabled infrastructure or a wider table-top exercise. On specific topics, virtual trainings could be envisaged. In terms of participation, greater involvement of the private sector should be foreseen.

4. Workshop proceedings

The workshop took place in Singapore on 6 and 7 June 2024, at the ASEAN-Singapore Cybersecurity Centre of Excellence, and benefitted from the participation of representatives from 17 ARF participating States (annex 2). The agenda was planned around 4 panels involving expert speakers from across ARF participating States, as well as interactive sessions and a tabletop exercise that focused on drawing out some of the learning points from the panel discussions.

Panel 1/ Interactive Session 1
Setting the Scene – Existing and Emerging Threats to ICT-enabled Critical Infrastructure.

Over the past two decades, the UN General Assembly's First Committee on Disarmament and International Security and regional organisations such as the Association of Southeast Asian Nations (ASEAN) and its Regional Forum (ARF) have provided vital platforms for the international community to exchange on responsible State behaviour in cyberspace. Despite progress, State and non-State actors continue to engage in malicious activities, often putting at risk ICT-enabled critical infrastructure, including those delivering essential public services.

Moderated by Singapore, speakers from Indonesia, Republic of Korea and Canada presented views on the most prevalent cyber threats affecting ICT-enabled critical infrastructure in their respective countries/region today, providing concrete examples of the different sectors affected, and specific policies and strategies that their governments have put in place in response.

Speakers shared a similar assessment of cybersecurity-related threats affecting critical infrastructure, which are increasing in number and sophistication. They also discussed new threats, such as the placing of malicious software or backdoors within critical networks to be activated in times of crisis or conflict. Such pre-positioning activity can lead to uncontrolled spill over, impacting non-targeted systems and potential escalation.

National cyber strategies have been developed over the past ten years in response, as have specific bills on the protection of critical infrastructure. These tend to be technology neutral, easily adaptable to changes in their uses. Speakers noted that the CI sectors most affected by cyber security incidents include government administration; healthcare, finance, ICT/telecommunications; energy and transportation.

Additional challenges that governments face include the nature of some of the key private companies (large multinationals registered in other jurisdictions), shortages of skilled personnel, regulatory uncertainty, low regulatory compliance, and oft-conflicting political and economic interests. Speakers also noted the difficulty of sustaining interest at the highest levels of decision making, since cybersecurity is still often seen as a technical topic and not sufficiently integrated into security, defense and development policy.

Governments are responding to CI-related cybersecurity threats by strengthening CII-related regulations and guidance, especially where CII asset identification is concerned. Speakers also noted the importance of investing in human resources, capacity building and in developing and disseminating cybersecurity maturity assessment guidance is important. Ongoing efforts to strengthen incident and crisis management and response through the establishment of coordination and communication protocols and platforms also aim to address cybersecurity threats and mitigate risks against CI.

Speakers and participants placed significant emphasis on the role of national and sector-specific CERTs and CSIRTs in responding to cybersecurity threats and vulnerabilities, and on the importance of continuously investing in building their capacity. They also discussed the role of national

CERTs/CSIRTs as critical nodes in notification and reporting of identified threats. In many contexts, recent legislation has included reference to these technical bodies, thus enhancing their importance in the cybersecurity response chain and allowing for greater allocation of resources.

Speakers also discussed how advances in technologies such as AI, Internet of Things (IoT), and 5G are impacting the threat landscape for critical infrastructure and how certain uses of these technologies can present opportunities for ICT-enabled critical infrastructure. Speakers noted that there are certain new/ emerging technologies (e.g., quantum) that we should already be thinking about from a normative and confidence building perspective.

Panel 2/ Interactive Session 2
Deep dive: Cybersecurity of OT for ICT-enabled Critical Infrastructure

The second panel of the workshop centred on cybersecurity of OT for ICT-enabled infrastructure. Moderated by the EU project *Enhancing security cooperation in and with Asia* (ESIWA), the panel included speakers from Cambodia, Singapore, Thailand and the United States whose remarks focused on the primary cybersecurity threats facing Operational Technology (OT) systems in industrial settings, such as manufacturing plants, power generation and distribution facilities, water treatment plants, and other critical infrastructure. Speakers shared lessons experienced on cyber incidents affecting OT systems. They explored some of the challenges arising from the convergence of OT and IT systems, as well as that of OT and IoT (commonly referred to as IIoT),[1] including challenges related to security (e.g., an increased attack surface, vulnerabilities in legacy OT systems, IoT device security), integration complexity (e.g., compatibility of disparate systems, data integration), governance and compliance (e.g., regulatory requirements and related costs, data privacy), and to cultural and organizational issues (e.g., obstacles to collaboration, differing objectives and priorities), amongst other .

Emphasis was placed on the role of government ministries and agencies in ensuring measures are put in place to monitor, detect, prevent, mitigate, and respond to threats, especially given the growing incidence of ransomware attacks. Speakers also considered how closer public-private engagement can enhance the management of physical and cyber security risks associated with integrated OT and IT/IoT systems.

One of the speakers proposed strengthening cybersecurity of OT in critical infrastructure from the perspective of people, process and technology. Such an approach can help overcome persisting challenges such as traditional mindsets, poor cybersecurity skills, and over-reliance on external service providers (people); poorly articulated CI-specific cybersecurity needs; an absence of context-specific guidance for OT stakeholders; and limited proprietary service support (process); a lack of basic cybersecurity controls; and poor adoption of cybersecurity-by-design (technology).

Speakers discussed some of the steps their countries are taking to overcome such challenges, some of which mirror those discussed in Panel 1. For instance, they highlighted the roles that CERTs and CSIRTs play alongside CI operators' security teams and relevant government actors to create an ecosystem of trust and transparency, which is indispensable to enabling greater cooperation between public and private sectors. They also insisted that a deeper understanding of the threat landscape can improve threat prioritisation, while also noting that government priorities – particularly national security ones – do not always align with the priorities of the private sector. As with other panels,

[1] IIoT is the use of smart sensors, actuators and other devices, such as radio frequency identification tags, to enhance manufacturing and industrial processes. These devices are networked together to provide data collection, exchange and analysis. Insights gained from this process aid in more efficiency and reliability. Also known as the industrial internet, IIoT is used in many industries, including manufacturing, energy management, utilities, oil and gas.

emphasis was placed on ensuring integration of after-action learning and reporting into these processes.

The panel was followed by interactive break-out group discussions on cyber security for OT during which facilitators and participants shared national experiences on the threat landscape. They also described the frameworks and mechanisms (including legislation, strategies, guidelines, and the establishment of national cyber security centres) that have been established at national level to identify and respond to threats, and which require dedicated budgetary allocations and qualified personnel.

Participants discussed the role of private sector companies in threat detection and mitigation and the importance of their adherence to requirements and guidelines at national level, of establishing their own cybersecurity processes and of ensuring skilled personnel at technical level. The latter is particularly difficult for small and medium-sized enterprises, therefore additional government support might be required. Incentivising interest in cybersecurity as a profession from a young age was discussed as a first step, and basic coding and programming should be introduced into curricula at all levels of education.

Cybersecurity regulatory frameworks were discussed during the break-out groups, with one group in particular emphasising the 'duty of care' principle regarding the roles and responsibilities of government actors in responding to CI-related threats. Others include governments' responsibility for establishing whole-of government cybersecurity-related coordination mechanisms, in ensuring that the cybersecurity of OT is reflected in government policy and guidance on cyber-security and incident response.

Participants once again emphasised the critical role of CERTs/CSIRTs as critical nodes in reporting and notification of identified threats and in responding to incidents, as well as the importance of investing in related capacities and capabilities. Some governments (e.g., through a national SOC) support raising awareness to ensure critical sectors are aware of trends in cybersecurity threats and the information and assistance that may be available to them through participation in specialised communities and fora, and at international level. Being connected to such forums and communities is key for exchanging information, identifying common TTPs (tactics, techniques and procedures) and indicators of compromise (IOC) and maintaining relevant data bases.

Public-private collaboration for managing security risks/incident response associated with cyber security threats in OT or integrated OT/IT systems is important. However, participants voiced concerns about persisting challenges such as the absence of trust to ensure effective public-private engagement, and the skills gap in OT cybersecurity, a challenge that is common to all countries. To foster greater trust and incentivize collaboration with the private sector, participants suggested that governments invite relevant companies to regular meetings to discuss cybersecurity challenges and regulatory concerns and that they establish regular procedures for communicating with and notifying companies of threats identified by national cybersecurity entities. Other possible incentives for strengthening relations with the private sector include: ensuring greater clarity on government mandates and regulatory requirements or obligations, consultations in the establishment of certification programmes, economic incentives for companies that meet cybersecurity standards, development of trusted platforms for information sharing and exchanges on OT threats and vulnerabilities; and sponsoring of education and training programmes focused on OT cybersecurity for employees in the public and private sectors.

Panel 3/ Interactive Session 3
Evolving Approaches to Risk Management for Resilient ICT-enabled Critical Infrastructure.

The third panel of the workshop centred on evolving approaches to cyber risk management for resilient ICT-enabled critical infrastructure. Moderated by the European Union, the panel included speakers from Brunei, the European Union, the Philippines and the United States. In their remarks they provided examples of how cyber risk management for ICT-enabled critical infrastructure is considered in private organisations and in national and regional cybersecurity policy and practice; the differences between reactive and proactive approaches to risk management; and the importance of ensuring a systems-based approach to risk management, which, as noted by one speaker, refers to understanding and addressing risks within an entire system, rather than just an isolated incident. Importantly, the latter entails continuous consideration of dependencies and inter-dependencies within a given organization in order to identify, assess and mitigate risks holistically.

More specifically, the session explored the different elements of risk management, including asset identification (e.g., enterprise, software, service providers assets), threat identification and prioritization, protection and recovery, and post-incident/after-action learning. Importantly, they stressed the importance of ensuring the adaptability of risk management frameworks to changing circumstances and technology, and for ensuring that lessons learned from prior incidents are taken on-board. Risk management maturity differs across sectors, with the financial services sector considered the most advanced at present in approaching risk management from a systems-based approach, and in considering dependencies and interdependencies in risk modelling.

Speakers discussed specific approaches to assessing cyber risk relevant to CI, and the different steps in the risk management process. A cyber risk matrix is often used in the initial steps of the process. Some such matrices apply a simple calculation of *cyber risk = scale of probability x impact*. Another approach involves analysing the *targeted asset* (e.g. a customer database, financial transaction systems etc.) against a *description of possible risks to the asset*, and then calculating its *scale of priority* in terms of *probability*, *impact* and its *risk value*. The next step is then evaluated in order to identify *risk mitigation options*, which can stem from existing standards or regulation, or determine whether the risk is 'transferred' through other means (e.g., via insurance coverage). Such approaches to risk management help prioritise spending on the basis of the highest risks and baseline security measures, some which stem from international standards and national regulation.

Speakers also discussed commonalities and differences in approaches to cyber risk management across various sectors, including energy and the financial services sectors, highlighting existing and emerging practices, and sector-specific challenges, including limited resources, knowledge and capacity for implementing risk management strategies. The importance of public private collaboration and stakeholder engagement was strongly emphasised, as were international cooperation and regular exchanges and exercises involving practitioners, policy and diplomatic experts on lessons learned and on new innovative practices in managing risk.

The panel was followed by interactive break-out group discussions on risk management for resilient ICT-enabled infrastructure, during which participants discussed in more detail on their respective national experiences in risk management. These included insights into challenges that derive from new legislative or complex regulatory requirements that are placed on operators relevant to risk management, and the difficulties encountered in meeting new standards. To avoid such challenges, early consultation with relevant stakeholders on regulatory changes is important, as is the timely publication and dissemination of guidelines when new regulatory requirements are established.

Suggestions on asset identification and prioritisation were discussed, including with regard to establishing relevant databases and regularly updating them. Regularly updated asset databases can serve as a basis for conducting regular threat assessments and putting in place more structured communication channels between the public and private sectors on threats and vulnerabilities.

The break-out groups reemphasised the importance of establishing sector-specific CERTs/CSIRTs alongside national ones and the importance of public-private data sharing, for instance between national SOCs and CI sector CERTs/CSIRTs or information security teams. To this end, several government representatives noted the utility – and urgency - of establishing secure information and threat data communication channels and information sharing platforms and bulletins.

Another identified good practice relates to public-private engagement when developing risk management strategies and assessments of dependencies and inter-dependencies. To facilitate these relations, it is important that governments put in place coherent coordination and consultations structures and designate points of contact at policy, regulatory and technical levels. The latter should be established in tandem with incident and crisis management protocols and procedures (e.g., for incident notification and reporting; security and threat awareness raising; and for international cooperation on incidents).

It was noted that risk management frameworks need to be dynamic, anchored in a systems-based appreciation of risk and capable of adapting to new threats and vulnerabilities and to technological developments.

Panel 4/ Interactive Session 4
Critical infrastructure resilience and the Framework for Responsible State Behaviour negotiated at the United Nations

The fourth and last panel of the workshop focused on CI protection and resilience in discussions at the United Nations General Assembly's First Committee on Disarmament and International Security and in the resulting framework for the responsible behaviour of States in their use of ICTs. Moderated by the EU, the panel included speakers from Singapore, Malaysia, the European Union and Australia.

Specific norms mentioned during the session include norms 13 (f), (g) and (h) from the 2015 GGE report of the UN Group of Governmental Experts (GGE), under which additional explanatory text was added in the 2021 GGE report. These norms form part of the framework of responsible behaviour of States in their use of ICT, which continues to be advanced within the current OEWG. The norms should be considered in conjunction with all other recommendations in the reports of previous GGEs and the first Open-Ended Working Group (OEWG). All speakers encouraged participants to read these reports that provide concrete actions for implementation and guidance on CI protection, amongst other

Speakers discussed their national and regional experiences in implementing the UN voluntary norms related to critical infrastructure, and in promoting adherence to the norms. Speakers considered how agreed confidence-building measures, as well as ones under consideration (such as the global directory of Points of Contact (PoCs)), can support the implementation of the critical infrastructure-related norms at the national level. One of the speakers presented a table with step-by-step guidance for implementing each of the key CI-specific norms agreed at the UN and the capabilities and capacities required to support implementation (Annex 3). For instance, CERTs/CSIRTs were identified as a core capacity for providing training and exercises to CI/CII sector leads. The proposed Global Point of Contact (PoC) directory was also presented as an important opportunity for facilitating more structured exchanges between states on the cybersecurity threat landscape.

One speaker recalled that while the agreed norms are voluntary, and efforts to implement the norms should take into consideration regional specificities. The importance of transparency measures relevant to responsible State behaviour was also highlighted. Such transparency measures can include publicizing national cybersecurity frameworks and policies; issuing public statements on capabilities and the conditions under which they would be deployed, and publicizing national views on how international law applies to cyberspace and the use of ICTs by States.

Speakers also considered ways to leverage operational expertise to inform diplomatic discussions on the security and resilience of ICT-enabled critical infrastructure. For instance, organizing multi-stakeholder consultations pre- and post-OEWG at national level to gather perspectives from owners and operators of CI and vendors of related services; cybersecurity firms or individuals providing services to CI clients; or regulators of CI sectors. Engagement of academia is often key as they can serve as a bridge between different stakeholders on CI-related discussions.

Finally, speakers highlighted the remaining effort needed to mainstream cybersecurity-related issues into multilateral and regional discussions, notably those focused on economic development and security.

Table-Top Exercise

The table-top exercise (TTX) centered around a disruption of ICT-enabled energy infrastructure owned and operated by a private company and affecting supplies in a fictitious country, as well as in neighbouring country. The TTX provided participants with the opportunity to further discuss and apply some of the lessons and takeaways from the workshop.

Key questions explored during *Phase 1* of the Exercise included: relevant crisis management and information sharing protocols and procedures, including the importance of government and industry PoCs for smooth communications between the CI entity and the government; the information to be included in the incident notification schema; the mechanisms and procedures governments can use to communicate with other governments or partners affected by the incident; and the procedures for communicating with/informing the general public at different phases of the incident.

Phase 2 of the Exercise focused on issues relevant to incident response and recovery, including the general or sector-specific policies, mechanisms or procedures that need to be in place to respond to incidents. Discussions considered the roles and responsibilities of different government entities when investigating incidents and the factors or information that would need to be considered if the government were to publicly attribute the incident. In terms of future preparedness, participants discussed the different elements of information that needs to be considered in an after-action review to evaluate the effectiveness of the response effort and ensure lessons are integrated into future risk assessment and incident management.

— end of report —

Annex 1 - Concept Note/Agenda

Folio 1_ARF
Workshop on Protecti

Annex 2 - List of countries that participated in the Workshop

List of Participating Countries
Australia
Bangladesh
Brunei Darussalam
Cambodia
Canada
European Union
Indonesia
Japan
Laos
Myanmar
Philippines
Republic of Korea
Singapore
Thailand
Timor-Leste
Russia
Vietnam

Annex 3 –Table of voluntary norms of responsible State behaviour relating to ICT-enabled Critical Infrastructure

DO NOT DAMAGE OTHERS	PROTECT YOURSELF	HELP OTHERS
• (f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;	• (g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;	• (h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

Annex 4 – Post-Workshop Survey and Key-Takeaways (Summarized)

- The majority of participants noted that Session 3: Evolving Approaches to Risk Management for Resilient ICT-enabled Critical Infrastructure, was most relevant to them.

- Key takeaways from the sessions included the importance of building regional cooperation on ICT security for critical infrastructure and ensuring a two-pronged approach: (i) Standardization, including sharing of best practices and establishing common baselines for ICT security measures across ASEAN member states; and (ii) Capacity Building, implementing workshops and knowledge sharing initiatives that can help member states identify their critical infrastructure and develop tailored risk management plans. The workshop also outlined the importance of Risk Management for organizations and discussed how to manage risk assessment and convey knowledge on OT Cybersecurity for ICT-enabled Critical Infrastructure

- Some participants suggested that focus areas such as countermeasures for protecting ICT-enabled critical infrastructure (IOT, Big data, Cloud computing) and technical presentations, e.g. on sectoral cyber security challenges (securing financial infrastructure vs energy infrastructure), could be included in the next round of workshops.